Access 5 Project Office
NASA
P.O. Box 273
Edwards, CA 93523 USA
661-276-2440
661-276-3880 FAX
www.access5.aero

COVER SHEET
Access 5 Project Deliverable

Deliverable Number: *CM001*

Title: *Contingency Management Requirements Document, Preliminary Version*

Filename: *CM001_Contingency Management Requirements_RevF_FINAL.doc*

Abstract:

This is the High Altitude, Long Endurance (HALE) Remotely Operated Aircraft (ROA) Contingency Management (CM) Functional Requirements document. This document applies to HALE ROA operating within the National Airspace System (NAS) limited at this time to enroute operations above 43,000 feet (defined as Step 1 of the Access 5 project, sponsored by the National Aeronautics and Space Administration).

A contingency is an unforeseen event requiring a response. The unforeseen event may be an emergency, an incident, a deviation, or an observation. Contingency Management (CM) is the process of evaluating the event, deciding on the proper course of action (a plan), and successfully executing the plan.

Status:

WP – Work in Progress Draft

Limitations on use:

This document is an interim deliverable reviewed and approved through the Contingency Management work package team and the SEIT. It is the analysis on contingency management supplied to the Policy IPT for their work in the creation of the Abnormal/Emergency operations position paper. It represents the project position on the top level functional requirement. Recommended lower level requirements and performance guidelines have not been validated at this time via the necessary simulation or flight test. In addition, the requirements have been limited to enroute operations above FL430 per the Step 1 definition of the Access 5 Project. Operations below FL430 and terminal operations have not been addressed in this document.

WORK PACKAGE 5
CONTINGENCY MANAGEMENT

CONTINGENCY MANAGEMENT REQUIREMENTS DOCUMENT (Preliminary Version)

September 30, 2004
(Revision F – 09/30/2005)

The following document was prepared by a collaborative team through the noted work package. This was a funded effort under the Access 5 Project.

Change Control Record				
REV	**DATE**	**AUTHORITY**	**CHANGE DESCRIPTION**	**APPROVED**
Orig.	30 Sep 04			
A	09 Feb 05		Incorporate IPT and Work Package Comments, Correct Errors	
B	25 Feb 05		Incorporate SEIT Review (18FEB05) Comments	
C	23 Mar 05		Delete Appendix C (Analysis of CONOPS and FRD). Correct associated tables and references.	
D	31 Mar 05		Add a different Appendix C (Multiple Failures). Add Appendix D (Onboard Systems Failures, CCA Failures Abnormal/Emergency Termination of Flight). Incorporate info from 15-17 Mar mid-project review.	
E	09 Sep 05		Incorporate comments from SEIT Webex of 29APR05, and from IPT/ Work Package Team Members. Incorporate guidance from the year-end review of 23-26 Aug 2005. Provide requirements traceability to the Access 5 Functional Requirements Document	
F	30 Sep 05		Add Appendix F Control Station Abnormalities. Revised the footnote conventions	

Signature Page

Karen Joerding Date

Systems Engineering and Integration Lead

Jim Evans Date

Technology Lead

Bernie Schmidt Date

Contingency Management Work Package Lead

TABLE OF CONTENTS

Section **Page**

LIST OF FIGURES

EXECUTIVE SUMMARY

A contingency is an unforeseen event requiring a response. Contingency Management (CM) is the process of evaluating the event and applying the necessary action to eliminate or minimize loss of life and equipment. Contingencies fall into one of three major categories, airborne failure, communication failure, and diversions. Control link failure, a subset of the communication failure, is shown to be the most troublesome of all contingencies, simply because the pilot loses his ability to send commands to the aircraft, and when he/she is not able to control the aircraft, it is impossible for the pilot to react and take corrective actions on a real-time basis.

The top level requirement for contingency management is:

The UAS System shall be capable of performing contingency management to reduce the likelihood of loss-of-life or damage to personal property at an equivalent level of safety comparable to manned aircraft.

Next level down from the top level requirement are five Contingency Management Functional Requirements:

1. The Air Vehicle Element shall operate safely and predictably in a manner equivalent to manned aircraft while performing emergency procedures.

2. In the presence of failures and abnormal events that degrade continuous and full time operator control of the UAS, the Contingency Management System shall provide related means to reduce the likelihood of loss-of-life or damage to personal property.

3. In the presence of failures and abnormal events that degrade SA (Situational Awareness) of the UAS, Contingency Management shall provide related means to mitigate and circumvent in to reduce the likelihood of loss-of-life or damage to personal property.

4. As part of any Contingency Management activity, the UAS System shall always have a recovery location identified in any route it may be flying.

5. The UAS System shall always have the means to safely terminate a flight.

A multiple failure is the presence of more than one single, independent, non-related failure at the same time during the same flight. When and if multiple failures occur in manned aircraft, the pilot should be able to take corrective action based on what the manufacturer recommends in the flight manual. The same principle applies when the UAS experiences multiple failures as long as the control link is available. When multiple failures in the UAS include failures in the control link, the pilot loses his/her ability to send commands to the aircraft to mitigate the other failures, and thus is severely restricted in his/her ability to save the aircraft and to prevent causalities on the ground.

The UAS has a unique function not found in manned aircraft; (command the aircraft from a location outside of the aircraft). If that function is flight safety critical, then mitigation measures may be required if that function fails.

Section 1.0
INTRODUCTION

This is the High Altitude, Long Endurance (HALE) Remotely Operated Aircraft (ROA) Contingency Management (CM) Functional Requirements document. This document applies to HALE ROA operating within the National Airspace System (NAS). The requirements apply to Step 1 of the Access 5 project, sponsored by the National Aeronautics and Space Administration (NASA).

1.1 BACKGROUND

A contingency is an unforeseen event requiring a response. The unforeseen event may be an emergency, an incident, a deviation, or an observation. Contingency Management (CM) is the process of evaluating the event, deciding on the proper course of action (a plan), and successfully executing the plan.

Contingency Management is major factor in how Unmanned Aircraft Systems (UASs) will be operated in the NAS, as well as a factor critical to their acceptance. Contingencies and their management are in every UAS flight manual as well as in the design engineering environments of aerospace companies that produce them. Contingencies range in importance from very minor malfunctions aboard the aircraft to flight critical failures that threaten the aircraft's survivability or threaten the lives of people on the ground, while others occur completely independent of the health and status of the UAS such as weather or collision avoidance. Successful resolutions to contingency situations may require significant deviations from flight planned activities or may be as simple as changing the transponder code in response to an on-board fault. The events that cause a UAS System to respond with contingency management actions are well understood by the UAS industry, and this body of knowledge must be converted into functional requirements for their safe operation in the NAS.

UAS developers have devised a wide range of methods in order to deal with contingencies. Some require pilot input to take care of contingencies, while others rely on fully autonomous methods. The exact method of handling contingencies has been largely up to the developers, whose primary focus has been to address the Concept of Operations (CONOPS) of military missions in restricted airspace or combat theaters.

The functional requirements developed for UASs in the NAS must take into account the proliferation of shapes, sizes, weights, and performance characteristics of UASs, and arrive at a common and clear process for managing contingencies.

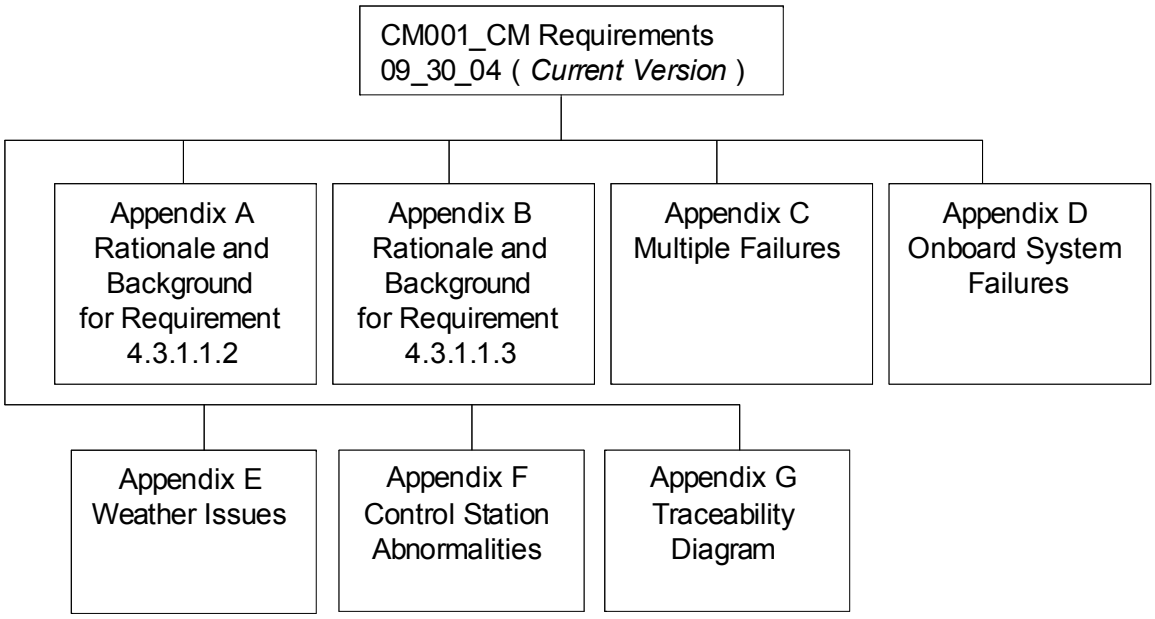
1.2 SCOPE

This document will discuss the events that can occur that require response, address the existing methodologies employed by UASs flying today to respond to these events, relate them to the Federal Aviation Regulations (FARs) for manned aircraft, and distill from them the functional requirements to be proposed for certification.

While in proceeding with this charter there are, in some instances, overlap with the assignments of other Access 5 work packages. This is unavoidable, and is being managed by constant communications with those areas and incorporation of their conclusions.

This document is the parent document for Appendices currently included and those under development. As revisions to the parent document and to any of the appendices are released, the Revision identifier attached to the parent document (i.e., Rev B, Rev C etc.) will be advanced and the appendices that are already released and not changed will also carry the new Rev identifier. This Rev identifier is noted in the header of every page, including the pages to the appendices. Whenever an appendix is revised, the entire CM requirements document and all of the appendices will carry the same Revision identifier even if some of the appendices have not been changed. The purpose of using this method is to always have a cohesive set of CM requirements that are in a single document.

The original was released on 30 Sep 2004, the current version is recorded in the Change Control Record on Page 2. Structure of the appendices:



Documents in addition to this CM Requirements Document are being produced by the Contingency Management Work Package. These additional documents are separate deliverables that are related to the parent document but not part of it. Those additional deliverable documents are:

Contingency Management Objectives and Scenario Definitions. Preliminary version was produced and delivered to the Technology IPT lead on 31 January, 2005. Revision A is scheduled to be released by the CM work package on 31 March, 2005.

Mission Planning Requirements Document. Preliminary version was produced and delivered to the Technology IPT lead on 28 February 2005. Revision A is scheduled to be released by the CM work package on 31 March, 2005.

1.3 PURPOSE

This document establishes System level requirements to facilitate CM for HALE ROA operating within the NAS. The document applies to the general HALE ROA industry, including defense, civil and commercial applications.

The requirements focus on functional capabilities for CM. The document discusses contingency events that can occur that require response, address methodologies employed by

existing UASs to respond to these events, and relates them to the Federal Aviation Regulations (FARs) for manned aircraft.

The requirements are stated in a design-and technology-neutral manner. That is, they are not dependent on the exact design or method for providing the functionality. On occasion, text accompanying a requirement may include examples of design or technology items intended for illustration only.

1.4 ACRONYMS / DEFINITIONS

1.4.1 Acronyms

ATC	–	Air Traffic Control
AVCS	–	Air Vehicle Control Station
BLOS	–	Beyond Line of Sight. Used interchangeably with OTH
C3L	–	Command and Control Communications Link
CCA	–	Cooperative Collision Avoidance
CM	–	Contingency Management
CONOPS	–	Concept of Operations
COP	–	Common Operating Picture
ELOS	–	Equivalent Level of Safety
FAA	–	Federal Aviation Administration
FCS	–	Flight Control System
FOD	–	Foreign Object Damage
FRD	–	Functional Requirements Document
FSS	–	Flight Service Station
IFF	–	Identification Friend or Foe
IPT	–	Integrated Product Team
LOS	–	Line of Sight
MITL	–	Man-in-the-Loop
NAS	–	National Airspace System
OEP	–	Operational Evolution Plan
OTH	–	Over the Horizon - Used Interchangeably with BLOS
SEIT	–	Systems Engineering and Integration Team
UA	–	Unmanned Aircraft
UAS	–	Unmanned Aircraft System

1.4.2 Definitions

Autonomous	–	Perform actions without human intervention. Having the ability to detect the contingency, evaluate the event, decide on the proper course of action, and execute the plan entirely without human intervention.
Command Chain	–	Total path that the command follows from pilot's intent to the component, module or subsystem on the UA that takes the final action. Command Link is a "link" in the Command Chain.
Command Link	–	The communications medium used by the UAS pilot to transmit commands from the AVCS to the aircraft. May also be referred to as "Uplink".
Contingency	–	An unforeseen event requiring a response. The unforeseen event may be an emergency, an incident, a deviation, or an observation.
Contingency Management	–	The process of evaluating the event, deciding on the proper course of action (a plan), and successfully executing the plan.
Pilot - ATC Comms Link	–	The voice radio communications method for the pilot to talk with ATC.
Return Chain	–	Total path that the signal follows from the component/module/ subsystem on the UA to the pilot's display. Return Link is a "link" in the Return Chain.
Return Link	–	The communications medium used by the UAS pilot to gain information and data on the health, status, performance, and intentions of the UAS. Telemetry is another word to describe what the return link provides. May also be referred to as "Downlink".
UAS Airport	–	Any airport that has been designated by the FAA as an Unmanned Aircraft airport. The criteria for an airport with this designation is fully described and covered in the UAS impact work package deliverable.

Section 2.0
PROCESS

The diagram below shows where the results of this work will be used. Output of the CM task teams have been incorporated into this functional requirements document, through the synthesis of the individual team's input and results. This document will be submitted and used by other IPT's and work packages in order to complete their FY-05 and subsequent work. The FY-04 document will also be used as a baseline for updates that will be the product analysis done by the CM work package during FY-05 and FY-06.

The interaction of task teams is important in ensuring that all contingencies and their ramifications in other areas is addressed

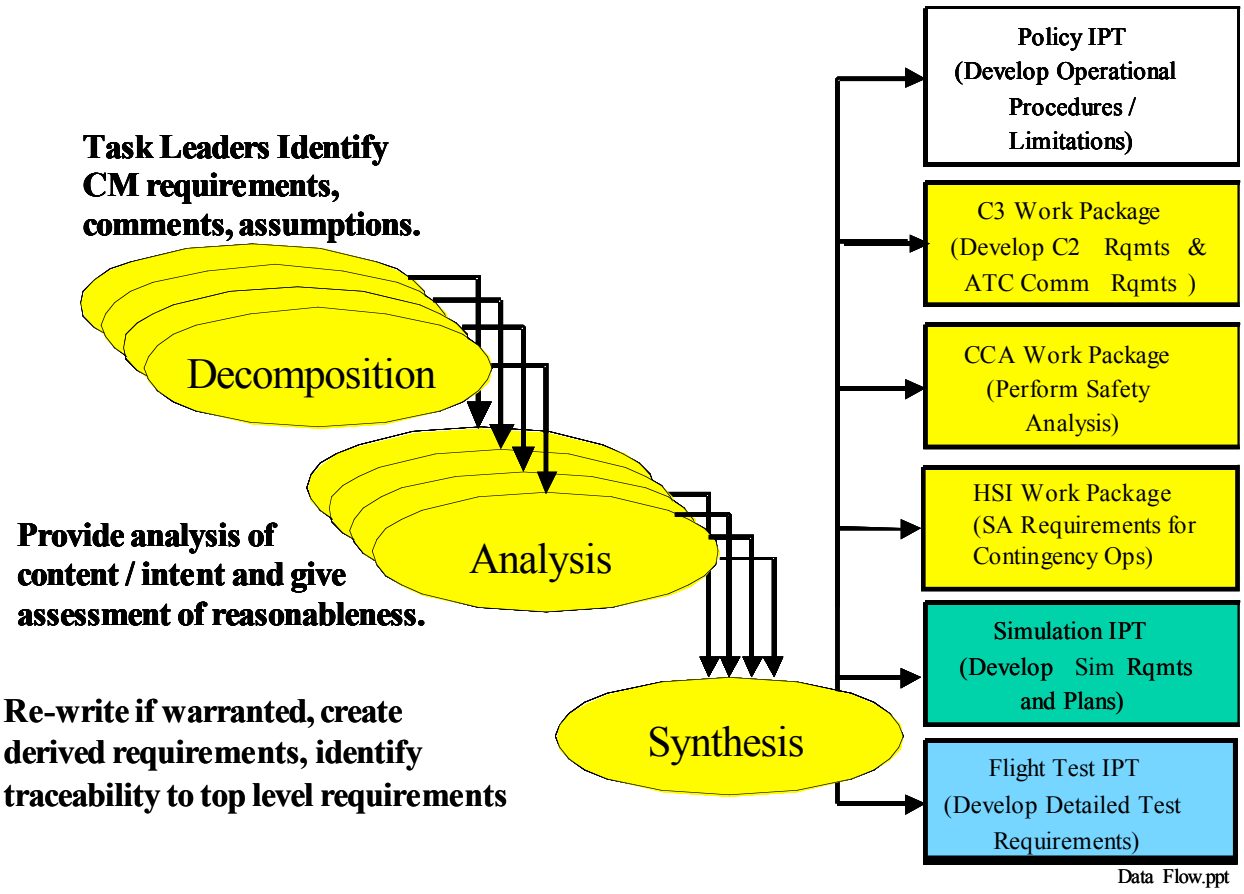


Figure 2-1. The Flow of Data and Information for the WP-5 (Contingency Management) Work Package

2.1 SEQUENTIAL STEPS TO ACHIEVING THE OBJECTIVES

The steps used by the CM Work Package team to arrive at the final requirements were designed to capture the analytical work performed by individual team members, and then sequentially synthesize those results. The steps were:

a. Identify and list all predictable contingency events.

b. Research literature and industry for methods and procedures being used to respond to these events in currently fielded systems.

c. Evaluate the technology currently available for this purpose and assess the practicality of implementing appropriate ones.

d. Leverage the knowledge and resources incorporated in the Access 5 CONOPS (Concept of Operations) and FRD (Functional Requirements Document).

e. Categorize the possible contingencies based on the similarity of their response actions.

f. Analyze these categories and the real events from which they are constituted to formulate functional contingency management requirements.

Section 3.0
OVERVIEW OF CONTINGENCY MANAGEMENT

3.1 FEATURES COMMON TO A TYPICAL UAS

3.1.1 UAS COP (Common Operating Picture)

The UAS Pilot obtains situational awareness from external sources, weather reports, traffic calls from ATC and other aircraft, and status information from airborne and ground observers. In addition, the pilot receives UAS health and status information directly from the aircraft through his/her return link. The total set of information is known as the COP.

In typical UASs today, the COP uses source information both from the pilot's knowledge base as well as information from the aircraft's knowledge base. This COP is available to the pilot and he/she is constantly able to affect the aircraft's behavior in response to changes in the COP.

3.1.1.1 Weather Awareness. No UAS's flying today are able to detect weather ahead nor, with flights lasting 34 hours or more, can anyone predict weather far enough in advance to ensure safety. While many environmental sensors are available, CM for weather avoidance currently depends on the pilot's weather situation awareness from external sources.

3.1.1.2 Collision Prediction and Avoidance. The current UAS has collision avoidance features that are imbedded in the pilot's decision making capabilities, based on the information that is supplied from a number of sources. On-board cameras on some UASs send imagery to the pilot’s displays and from there the pilot makes avoidance maneuvers. These cameras are useful during landings, takeoffs, and during ground operations for the purpose of avoiding ground obstacles. They have limited utility against airborne traffic. FAA controllers give traffic advisories in a manner similar to that which is done for manned aircraft. While the procedures and technologies for cooperative collision avoidance are being addressed in the CCA work package, collision avoidance for current UAS's is strictly a pilot function.

3.1.2 Contingencies and Flight-Planned Routes

As with manned aircraft, UASs follow a filed flight plan, called in the industry, the mission plan.

When a contingency requiring a deviation from the planned route occurs, the route is modified either directly by the pilot, automatically by the UAS, or through uploading new route software. The new route will take into account the nature of the contingency, and if the contingency is such that landing cannot be affected, a new route will be selected to avoid descending on a populated area.

3.1.3 Methods for Pilot Control of UAS'S

3.1.3.1 Manual (Direct Pilot-in-Loop) Remote Control. The ground-based pilot manages the UAS directly during taxi, takeoff and landing. During up and away flight the pilot controls the vehicle through autopilot modes. A reasonable amount of data is typically down linked to the pilot to provide status information and assist the pilot in emergency situations. If there is a temporary data link interruption and a failure occurs during the interruption, the pilot may not know about the failure until it is too late to make any potential corrections.

This method is still very popular with the industry since it is cost effective in many cases. The pilot commands direct movements to the flight control surfaces or monitors the auto-pilot that is programmed to fly a particular route. If the pilot must interrupt that plan, he/she manually sends commands up to the aircraft to re-direct the flight.

3.1.3.2 Autonomous Control. In this mode the UAS pilot typically gives the taxi start and stop commands and the takeoff command. The UAS follows the preplanned mission plan, unless an "override command" is received from the ground-based pilot. Some contingency management functions are typically included in the mission plan, but frequently require concurrence from the pilot. If data link communication to the UAS is lost, the pilot knows what the UAS's flight plan is and can contact the ATC to determine what squawk is being observed. If there is an additional emergency during the lost communication, the pilot might not be able to interact with the UAS. This method allows the aircraft to make decisions that are done without pilot input or approval. The pilot still has the ability to override those aircraft originated decisions provided a command link is available.

3.1.3.3 Autonomous Control and Autonomous Contingency Management. Such an UAS, during normal operation, behaves similar to the UAS in section 3.1.3.2. However, there are significant differences when an emergency is encountered. This type of UAS has the ability to select an alternate landing site, should an engine failure or some other failure require such actions. This in turn requires alternate status communication paths should such action be taken when the command and status link between the ground-based pilot and the UAS are lost. The key item will be to define the allowable probabilities of such actions.

3.2 CURRENT CONTINGENCY MANAGEMENT CONCEPTS AND IMPLEMENTATION

Categories have been created to accurately depict the current state of contingency management. The three categories that describe their defining characteristics are below, and examples of current contingency management for four UAS systems are presented in table format after that. These examples are ones that could be expected during the life of any particular UAS, described for a current UAS, and the most likely contingency actions to mitigate the failure. Additional analysis of those typical contingencies, and the current methods for handling them, provides rationale of how this particular instance justifies the requirements in Section 4.0.

Likely contingencies have been grouped into three categories. The three categories and defining characteristics are:

A. UAS Airborne Segment Problems or Faults Defining Characteristics:

1. Involves the airborne segment as the failed component.
2. Uses Advisory Circular (AC) 25.1309-1A, System Design and Analysis, paragraph 6h to describe severity of the failure condition. The severity ranges from Catastrophic to Major to Minor.
3. Involves typical scenarios from actual experience of fielded systems.
4. Describes reasonable or expected circumventing and mitigating processes.

B. Communications Failures Data Link Failures Defining Characteristics:

1. This sub-category is established since these types of contingencies and the mitigation measures should be treated differently from the more familiar airborne failure contingencies.
2. Communications failures do not fit into the AC 23 and 25.1309 guidance and applicability concepts since the AC's primarily focus is on the assumption that humans are always aboard the aircraft.
3. The AVCS is an integral part of the failure condition.
4. Simultaneous failure of an airborne sub-system and the data link system falls into this category. (Probabilities of simultaneous failures have not been established.)

Pilot and Controller Communication Failures Defining Characteristics:

1. The contingencies involve interaction with entities outside of the UAS system.
2. Lost Comm contingencies have a proven, simple set of procedures that are well understood and straightforward for manned aircraft. However, those procedures in the Airman's Information Manual (AIM) Par 6.4.1 and in other FAA documents will need to be modified to allow for peculiar UAS requirements.

C. Diversions Defining Characteristics:

1. This category addresses abnormal operations using fully functioning UAS systems.
2. Examples of diversions are go-arounds during approach, collision avoidance maneuvers, weather avoidance, etc.

3.2.1 Current Contingency Management with Airborne Segment Failures or Faults

Figure 3.2.1-1 depicts the normal sequence of events when failures occur on the UAS platform.

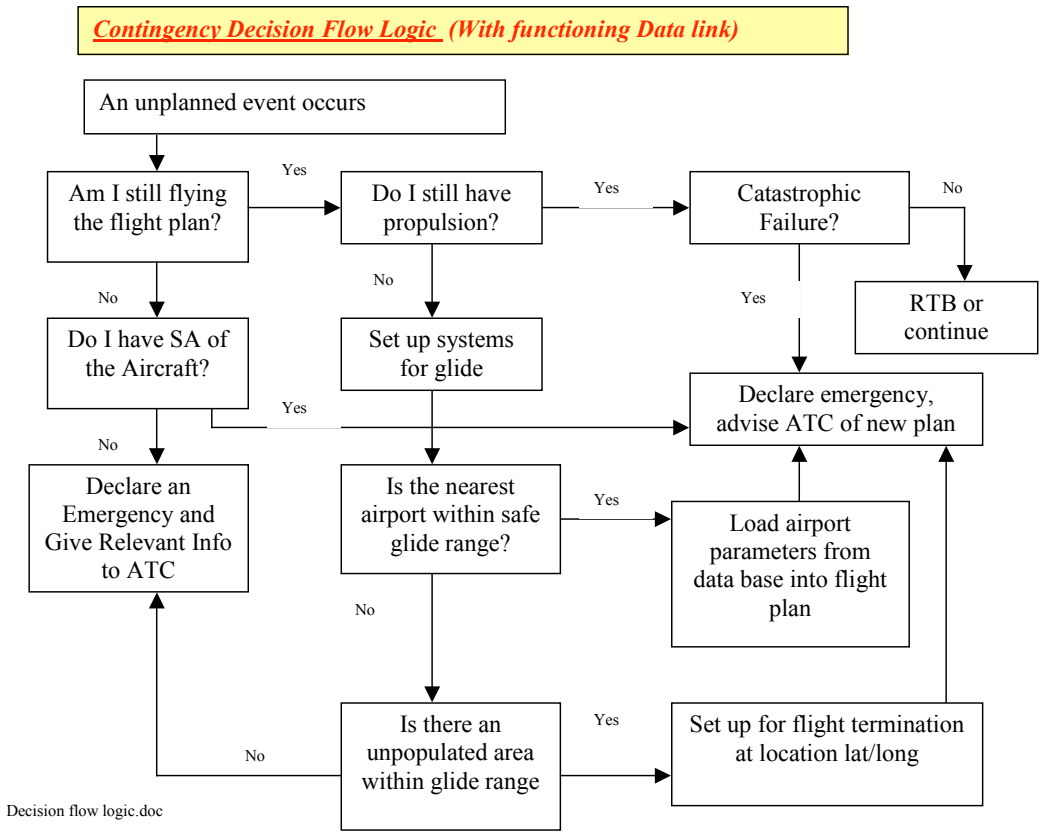


Figure 3.2.1-1. Normally the UAS Follows This Logic Sequence for Airborne Failures with a Functioning Data Link.

3.2.1.1 Catastrophic Failure. A failure condition that would prevent continued safe flight and landing (AC 25.1309-1A). UAS would experience the "Effect on Airplane" of Hull Loss, but would not affect crewmembers or occupants since the UAS is unmanned. Loss of life would apply only to people on the ground or in the other aircraft in the event of a midair collision.

Figures 3.2.1.1-1 and 3.2.1.1-2 provide examples of currently operating UASs that might experience a catastrophic failure.

Example of Catastrophic Failure: Engine Failure With a Single Engine UAS	
UAS	**Contingency Management Actions**
Global Hawk	Aircraft automatically switches to a different route and follows that route to a location and lands. Battery life is limited with engine off so the landing location must be within the flying range on battery power. Aerodynamically, the aircraft will exceed that range. Transponder modes and codes are changed.
Helios	No data supplied.
Perseus	Pilot has to feather the Propeller to achieve the L/D of 18. The pilot must decide to RTB or land off field. Pilot has to modify the auto-navigation route or switch autopilot modes to heading hold or bank hold to RTB. Landing is performed pilot in the loop, unless the LOS link is lost, in which case it will maintain a set heading and airspeed until touchdown. Battery life is 1 hour under normal loads. Transponder modes and codes can be changed by the pilot.
Predator	UAS pilot reports event to ATC. Alternate comm. path (Land Line etc.) may be used when aircraft is at lower altitudes or when link is lost. Electrical load shedding of non-essential sub systems and equipment items will be executed. Multi battery system has capacity sized for descent from high altitude plus reserve. This permits continued operation of essential functions including ATC radio, Transponder and Data Link. Non-Recoverable Engine Out With Operational Data Link: Aircraft descends under pilot control to a pre-determined point as defined in mission planning. For all mission segments the mission planning accounts for an engine-out landing at the nearest airfield or an emergency set down when this is not available. The latter is selected to avoid bodily harm and loss of life. Non-Recoverable Engine Out Without Data Link: Aircraft descends under air vehicle autopilot managed Emergency Mission to a pre-determined set down point. Emergency Mission is loaded prior to flight and derives set down points from the mission planning phase for all flight segments to avoid bodily harm and loss of life. Emergency Mission is also capable of being pre-programmed to affect Transponder response (modes & codes).

Figure 3.2.1.1-1. Engine Failure With a Single Engine UAS

Example of Catastrophic Failure: Structural Failure During Flight Causing Loss of Control	
UAS	**Contingency Management Actions**
Global Hawk	Air vehicle descends in the out-of-control state and impacts the ground below the aircraft within a circular area with a pre-determined radius. TRANSPONDER squawk automatically changed to 7700.
Helios	
Perseus	If FTS (Flight Termination System) equipped, the will be activated. Air vehicle descends under the parachute and impacts the ground within a circular area with a pre-determined radius dependent on the initial altitude. The transponder can be changed to squawk 7700.
Predator	A projected ground set down area is displayed in the Ground Control Station. This is based on vehicle states and boundaries from a platform specific descent model. Transponder, flight computer and system support batteries located to maintain transponder operation to circumvent separation of major airframe components (Wings, Empennage, Propulsion etc.). UAS pilot reports event and details to ATC. Alternate comm. path (Land Line etc.) may be used when link is lost. Pilot issues commands for propulsion shut down.

Figure 3.2.1.1-2. Structural Failure During Flight Causing Loss of Control

3.2.1.2 Major Failure. A failure condition which would reduce the capability of the airplane or the ability of the crew to cope with adverse operating conditions, for example:

A. A significant reduction in safety margins or functional capabilities, a significant increase on crew workload or in conditions impairing crew efficiency.

B. In more severe cases, a large reduction in safety margins or functional capabilities, higher workload, or physical distress such that the crew could not be relied on to perform its tasks accurately or completely, or adverse effects on occupants. (AC 25.1309-1A) For UAS, "occupants" does not apply.

Figures 3.2.1.2-1 through 3.2.1.2-4 are examples of major failures. The figures describe CM actions for these failures.

Example of Major Failure: Generator Failure	
UAS	**Contingency Management Actions**
Global Hawk	The AC generator powers the mission related equipment such as payloads and acts as a backup power source for aircraft functions such as comm gear, lights, flight controls, main computers, etc. If the AC generator fails, the aircraft continues on its current mission for a short time to allow the pilot to decide to continue or return to base. If no action is commanded, the aircraft automatically switches routes and proceeds to a pre-designated landing point. Payloads and non-flight critical equipment are automatically shut down and the DC generator powers an inverter that supplies power to the remaining AC powered equipment.
Helios	No data supplied.
Perseus	The aircraft is equipped with two DC generators. One powers the aircraft systems and one powers the payload and acts as a backup power source for the primary aircraft functions such as C3 links, lights, flight controls, flight computer, etc. If the primary generator fails, the Generator Control Unit will transfer the load to the payload generator. Payloads and non-flight critical equipment are automatically shut down. In the event of a generator failure the mission would be discontinued and the aircraft would RTB.
Predator	Loss or Degradation of Electrical Generator Within Range of Landing Site: The UAS has multiple redundant batteries sized to enable maintaining communications and essential aircraft functions for descent and landing plus reserve. Electrical load shedding of non essential sub systems and equipment items will be executed. Transponder and ATC radio will remain functional. Inform ATC of need for mission abort and recover and land UAS at the nearest landing site. Loss or Degradation of Electrical Generator Beyond Range of Landing Site: The UAS has multiple redundant batteries sized to enable maintaining communications and essential aircraft functions to for descent and landing plus reserve. Electrical load shedding of non essential sub systems and equipment items will be executed. Transponder and ATC radio will remain functional. Inform ATC of need for mission abort and descend and emergency set down to avoid bodily harm and loss of life.

Figure 3.2.1.2-1. Generator Failure

Example of Major Failure: Partial Flight Control Sub-System Fault / Degradation	
UAS	**Contingency Management Actions**
Global Hawk	Aircraft has redundant flight control surfaces and computers for controlling them. Gains are changed on the remaining flight controls to maintain stable flight. Depending on the importance of the failed components, the aircraft makes a decision to either continue with the flight or switch to a different route, containing waypoints and action points that are appropriate for the type of fault.
Helios	For each of these non-deferred emergencies, except loss of uplink at low altitude, the contingency action is to interpret what the problem is and return the aircraft to acceptable limits. A redundant FCS is available if the primary FCS does not appear to be operating correctly. For loss of uplink at low altitude, switching to the redundant FCS is the corrective action.
Perseus	The aircraft has redundant flight controls and sensors. The flight computer has the Fault Tolerant Control software which will allow the aircraft to maintain control within the flight envelope in the event of an actuator or sensor failure. The FTC software will detect the failed sensor and switch to the backup unit. In the case of a failed actuator, the FTC software will detect the failure and reconfigure the flight control laws. The pilot will command the aircraft to RTB.
Predator	Multiple failures of redundant core avionics (INS/GPS & Flight Computer Channels) are required in order for this to occur. Multiple failures annunciated in AVCS. Excluding rapid or common mode events, failures are likely to be in sequence with potential for mitigating action after first failure (RTB etc.) and prior to total loss of control. Nav. lights and the Transponder remain operational. Air vehicle is unable to maintain controlled flight. A projected ground set down area is displayed in the Ground Control Station. This is based on vehicle states and boundaries from a platform specific descent model. Relaxed stability circumvents uncontrolled fly away. Pilot issues commands for propulsion shut down. UAS pilot reports events and details to ATC. Alternate comm. path (Land Line etc.) may be used when aircraft is at lower altitudes or when link is lost.

Figure 3.2.1.2-2. Partial Flight Control Sub-System Fault / Degradation

Example of Major Failure: Stuck or Degraded Propulsion Setting	
UAS	**Contingency Management Actions**
Global Hawk	No data supplied.
Helios	No data supplied.
Perseus	No data supplied.
Predator	Abort mission and RTB or to recovery airfield followed by engine kill and engine out descent and controlled landing. Inform ATC of RTB and subsequent in-air engine out procedure and descent and landing at recovery airfield. The UAS has multiple redundant batteries sized to enable maintaining essential communications and aircraft functions to for descent and landing plus reserve. All essential functions including Transponder and ATC radio will remain functional after engine kill. Electrical load shedding of non essential sub systems and equipment items will be executed to facilitate this. Propulsion Setting Stuck at Low or Climb Setting within Range of Recovery Airfield. Abort mission and kill engine and perform descent and controlled landing at recovery airfield.

Figure 3.2.1.2-3. Stuck or Degraded Propulsion Setting

Example of Major Failure: Degradation of Navigation Function	
UAS	**Contingency Management Actions**
Global Hawk	No data supplied.
Helios	No data supplied.
Perseus	No data supplied.
Predator	Loss of main high fidelity INS/GPS sub system defaults to flight control triplex INS/GPS. This enables full aircraft function but will negate accurate pointing for wideband SATCOM antennas. This link system will therefore be unavailable. UAS will resort to low bandwidth SATCOM to maintain aircraft status and control for BLOS operation. Aircraft will likely need to RTB or nearest landing site due to reduction in situational awareness with inability to convey aircraft nose camera video while in BLOS mode. Video will again become available when in range of LOS system within approximately 125nm of AVCS site. UAS pilots report event and related status to ATC. Temporary Degradation Of Navigation. Temporary loss or degradation of the GPS signal will be circumvented by automatically maintaining navigation functions with the aircraft low drift INS system. Normal GPS assisted navigation seamlessly resumes when temporary loss or degradation of GPS signal is restored to normal levels. UAS pilots continue operation and mission as part of normal procedures.

Figure 3.2.1.2-4. Degradation of Navigation Function

3.2.1.3 Minor Failure. Failure conditions which would not significantly reduce airplane safety, and which involve crew actions that are well within their capabilities. Minor failure conditions may include, for example, a slight reduction in safety margins or functional capabilities, a slight increase in crew workload, such as routine flight plan changes, or some inconvenience to occupants. For UAS, "occupants" does not apply.

Figure 3.2.1.3-1 shows examples of minor failures.

Example Of Minor Failure: Non-Critical Sub-System Sensor Failure	
UAS	**Contingency Management Actions**
Global Hawk	One of the nine temperature probes fails. The remaining temperature sensors are used to synthesize the missing temperature reading by applying offsets. Notice is sent to the pilot.
Helios	The Minimum Equipment List (MEL) for critical sensors on Helios states each critical sensor is to be triple-redundant. Failure of a single critical sensor, defined as an out of bounds measurement, will not result in an immediate degradation to the aircraft's flight systems. Safe flight will continue with the remaining now dual-redundant critical sensor. An indication of the specific critical sensor failure will appear on the Ground Control Station. Because the critical sensor no longer meets the MEL requirement, the pilot will return the aircraft to base as soon as possible. A non-critical sensor or system failure may result in an affect on the aircraft in attitude, airspeed, or navigation, or may result in the inability to complete the mission. For Helios, non-critical sensors include: roll (roll rate), angle-of-attack, sideslip, vertical speed, and up link signal strength. Non-critical systems include: the aircraft data computers and transponder. In the case of non-critical sensor or system failure, intervention by the remote pilot is only required if the autonomous systems have insufficient information to work properly. If necessary, the remote pilot will use information from healthy sources to compensate for the failed non-critical sensor or system. The remote pilot will then evaluate of the severity of the effect of the non-critical sensor or system failure. Depending on the resulting effect of the failure, the remote pilot will decide either to continue the flight or to land.

Figure 3.2.1.3-1. Non-Critical Sub-System Sensor Failure (Sheet 1 of 2)

Example Of Minor Failure: Non-Critical Sub-System Sensor Failure	
UAS	**Contingency Management Actions**
Perseus	In the event of a single sensor failure, a caution or warning will be displayed on the master caution panel or a system information screen. The pilot will attempt to resolve the problem using the normal or emergency procedures. If the problem can not be corrected, the pilot will utilize other sensors to derive the information. This would increase pilot workload, but not affect safety or mission completion.
Predator	No data supplied.

Figure 3.2.1.3-1. Non-Critical Sub-System Sensor Failure (Sheet 2 of 2)

3.2.2 Current Contingency Management with Communications Failures

3.2.2.1 Data Link Contingencies. In the event of lost command and control, some UASs are programmed to climb to a pre-defined altitude until contact is re-established. The Global Hawk UAS is capable of making informed mission decisions to continue or to reroute to an alternative airfield without pilot assistance. For other UASs, if contact is not reestablished in a given time, the UAV can be pre-programmed to 1) retrace its outbound route home, 2) fly direct to home, 3) continue its mission, or 4) Climb, orbit and wait a pre-determined period of time prior to performing 1 or 2 above.

3.2.2.1.1 Lost Command Link Contingencies. Current UAS systems use a "Command Chain" to transfer the pilot's intent to the aircraft. The pilot's intent follows a path through a number of components in a serial arrangement. The pilot moves a control or mouse in the ground station, the command goes from there to a processor, thru modems to an antenna, to the satellite, to the antenna on the airplane, then through the aircraft's modems and processors until it arrives at the flight control surfaces on the airplane. Think of this functionally as the "command chain" rather than simply the data link.

There are times in the current UAS systems when the command chain is not available. For example, a satellite may be temporarily blocked by part of the aircraft structure. In that case, the pilot simply waits until the aircraft moves back into favorable coverage, or the aircraft takes an autonomous action to solve the problem.

Figure 3.2.2.1.1-1 shows examples of data link failures when the pilot is unable to send commands to the aircraft. The figures describe CM actions for these failures.

Example of Data Link Failure: Pilot is Unable to Send Commands to the UAS	
UAS	**Contingency Management Actions**
Global Hawk	Immediately at occurrence of the fault, the aircraft starts a timer that delays the aircraft's corrective action response. If there is no command to set the timer, it is defaulted to trigger automatically. This same timer applies to the status (downlink) as well. When the timer reaches its limit, the aircraft switches itself to a different route and flies the new route. It also executes action points on that new route, which are primarily related to re-acquiring the data link. As with all routes that are available and pre-programmed into the aircraft's nav system, the lost comm routes go to a designated touchdown point and land, waiting there for the ground personnel to shut off the engine and tow it off the runway.
Helios	Loss of the redundant up link signal strength would result in an effect on the aircraft only if a second failure of the primary up link occurred. In this case, protocol is to return to base and land as soon as possible, though an emergency would not be declared.
Perseus	If the flight computer does not receive an uplink status or command within 300 ms, then it arms the lost link mission. It will automatically switch to the lost link mission depending on the preset arming altitude. On the runway or on the upwind below 500 ft, it will kill the engine, set the airspeed to Vy (best rate-of-climb speed), engage bank hold and apply the brakes. It will fly straight ahead in that configuration until touchdown. Above 500 ft, the aircraft will begin navigating to the first pre-programmed lost link mission waypoint. It will also climb or descend to the initial lost link altitude. The aircraft will attempt to reestablish the link using the primary and secondary RX/TX antennas. Once in the lost link mission it will continue to fly the waypoints until the link is reestablished, the FTS is activated, or the fuel is exhausted and the aircraft descends to the surface. The pilot will follow the Lost link emergency procedures to attempt to reestablish the link. This will include switching transmitters, directional and omni antennas, or AVCS racks. The TRANSPONDER code will be the same as previously set.
Predator	The Lost Link response of the Predator system is dependant on the nature of the loss of the link. The three classes of Lost Link are described below. Total AVCS Loss - without a back up AVCS site Multiple failures of the redundant AVCS equipment are required to get to this state. The loss of the sole AYCS results in the loss of C2 data link and loss of the AVCS audio channel to the aircraft ATC radio. The aircraft flight computer program responds by immediately entering the Lost Link/Emergency Mission mode that flies pre-programmed way points (i.e. holding/loiter patterns) and eventually to a pre-determined set down point. The set down is executed after an extended period to minimize set down fuel state and to maximize the opportunity to re-acquire the C2 link(s). The Lost Link/Emergency Mission is loaded prior to flight and derives its set down points from the mission planning phase for all flight segments to avoid bodily harm and loss of life. The Emergency Mission is also capable of being pre-programmed to change the Transponder response (modes and codes etc.). The UAS pilot reports the event and related status to ATC via a back up communications channel (VHF/ATC radio or Land Line etc.). The aircraft navigation lights and transponder remain functional. Total Loss of All UAS Data Link Systems Total loss requires multiple failures in the redundant C Band LOS system, plus failure of the wide bandwidth Ku SATCOM link and failure of the low bandwidth IRIDIUM SATCOM link. Under these circumstances the aircraft autopilot function executes the following Lost Link/Emergency Mission sequence, whilst continuing to re-establish any of the available data links: a) 0-10 seconds.. The autopilot flies the aircraft. based on the last input command. The pilot receives a Lost Link warning in the AVCS.

Figure 3.2.2.1.1-1. Pilot is Unable to Send Commands to the UAS (Sheet 1 of 2)

Predator	b) At 10 seconds. The autopilot activates roll/pitch/yaw/airspeed holds and sets heading

Example of Data Link Failure: Pilot is Unable to Send Commands to the UAS	
UAS	**Contingency Management Actions**
	hold to the initial Lost Link heading. Then the autopilot increases the throttle to climb setting, if the aircraft is below a pre-programmed altitude, otherwise the throttle setting is maintained. The autopilot commands all unnecessary electrical loads to be shed. c) 1Osec-30min. The autopilot flies a circular loiter pattern of preprogrammed diameter and pre-programmed offset from the Lost Link Point in the direction of the Lost Link heading. d) At 30 mm. The autopilot begins to fly a course of pre-programmed way points (Emergency Mission Profile) until fuel runs out or a preprogrammed time limit expires at which time the autopilot lowers landing gear and initiates a controlled descent to a pre-programmed set down point. The loss of C2 causes loss of the AVCS audio channel to the aircraft ATC radio. The UAS pilots can report the situation to ATC via a back up communication channel (VHF/ATC radio or Land Line etc.). The Emergency Mission is also capable of being pre-programmed to change the Transponder response (modes and codes etc). Navigation lights and Transponder remain functional. <u>Loss of BLOS SATCOM Data Link Systems</u> Permanent loss of the Ku SATCOM system is cause for aborting the BLOS mission and returning to LOS range. The back up BLOS low bandwidth IRIDIUM SATCOM system will only support a voice channel to the ATC radio, reporting of aircraft telemetry and uplink of aircraft navigation waypoints and control modes. The IRIDIUM systems primary function is to allow continuation of the BLOS mission when temporary outages of the wide bandwidth Ku SATCOM system occur. The aircraft is managed, via the IRIDIUM SATCOM system, without the loss of the cruise function back in to range (125 nm) of the LOS system where nose camera video will be re-instated and normal recovery and landing can be executed. Permanent loss of the IRIDIUM SATCOM system may be cause for returning into LOS range depending on the mission type and safety assessment since full aircraft, C2 and ATC voice functions are provided by the Ku SATCOM system. Under both conditions described above navigation lights, ATC Radio and the Transponder all remain functional and the UAS pilot can report the event and related status to ATC.

Figure 3.2.2.1.1-1. Pilot is Unable to Send Commands to the UAS (Sheet 2 of 2)

3.2.2.1.2 Lost Return Link Contingencies. The objective of this section is to provide information about how current UAS pilots determine the intentions, status, and health of a UAS that is experiencing return link failure. The UAS pilot takes the necessary actions to assess the condition of the UAS as the result of this type of failure.

The technologies and processes that are available to provide health/status/intentions to the UAS pilot in event of loss of the return data link are limited to very few options. One option is to ask the ATC for assistance in some way. An example would be to request a TRANSPONDER check to determine if the transponder is functioning. Others are largely impractical in the NAS, such as following the UAS with a manned chase aircraft.

Figure 3.2.2.1.2-1 shows examples of loss of data link in the down direction (from the UAS to the Air Vehicle Control Station (AVCS). The figure describes CM actions for these failures.

Example of Data Link Failure: Aircraft and Ground Station Lose All Capability To Transfer Location and Status Information to the Pilot.	
UAS	**Contingency Management Actions**
Global Hawk	After the lost comm timer times out, the aircraft switches itself to a different route and now flies the new route to a landing, as long as no other faults or emergencies occur. The pilot is not able to receive any location or health status on the aircraft. It is not possible to determine if the command link is able to function since there is no feedback concerning commands being sent. The problem could be in any of the links in the chain of information (aircraft internal data flow, transmitter problems on the aircraft, receiver problems in the ground station, display problems in the ground station. The pilot could: 1. Check with a redundant ground station. 2. Notify nearby aircraft (military) to see if they can join in formation and determine what is happening. 3. Query the ATC agency controlling the aircraft and ask if ATC sees any transponder returns that indicate the aircraft's status such as 7600 or 7700.
Helios	Loss of the vertical speed data would be nearly irrelevant as long as GPS and pressure altitude data is still available. In the event of the loss of the transponder, ATC could perform a skin track.
Perseus	The aircraft will continue to fly along it's last commanded heading, altitude, airspeed or route. The pilot will attempt to regain the downlink by switching transmitters, directional and omni antennas, or AVCS racks. The position of the aircraft may be verified using the TRANSPONDER by the ATC radar controller or a range controller if the vehicle is equipped with a C band beacon. The Pilot will follow the lost downlink procedures. The pilot may be able to manually adjust the AVCS directional antennas to re-acquire the downlink. If the downlink is lost, the pilot may assume that the uplink is also lost. The TRANSPONDER code will be the same as previously set.
Predator	Same description as in "Pilot is Unable to Send Commands to the UAS" above.

Figure 3.2.2.1.2-2. Aircraft and Ground Station Lose All Capability To Transfer Location and Status Information to the Pilot

3.2.2.2 Lost Communications Contingencies. Most lost communications situations involve the breakdown of voice communications between the UAS pilot and the ATC controller. A straight-forward loss of this function is easy to resolve by making a telephone call. Current COA's require a phone number on the flight plan. This number is the UAS pilot's number where the controller or the supervisor can contact the pilot to re-establish communications. The pilot can also call the supervisor at the ATC agency that is controlling the UAS. A failed phone contact is a classic communications failure, and UAS vehicles follow the pre-planned mission instructions documented in 14 CFR 19.185. This procedure may need modification for UASs because the "Proceed in VFR" provision may not apply since the pilot is not in the aircraft.

3.2.3 Current Contingency Management Involving Diversions

3.2.3.1 Traffic Avoidance. Once the "see" portion of S&A is satisfied, the UAS pilot must use this information to execute an avoidance maneuver. According to FAA and DoD studies, the latency between seeing and avoiding for the pilot of a manned aircraft ranges from 10 to 12.5 seconds. If relying on a ground pilot to see and avoid, the UAS incurs the same or greater human latency, but adds the latency of the data link in bringing the image to the ground for a decision and then sending the avoidance command back to the UAS. The total system delay can

be as high as 16 seconds with satellite links. The 16 seconds is measured from the pilot first becoming aware of the problem to the first movement of the aircraft.

3.2.3.2 Weather Avoidance. As mentioned earlier, weather avoidance is currently embedded in the pilot's responsibility for safe conduct of the flight. All weather information is part of the COP that is maintained by the pilot who maneuvers the aircraft to avoid problems with weather.

3.2.3.3 Diversions During Flight on or Near the Airport. Current UAS's have a mix of capabilities depending on the level of autonomy that is designed into the system. For a strictly MITL (Man-in-the-loop) system, the commands must be transmitted to the aircraft after the condition is made known to the pilot. Autonomous aircraft are able to execute abort maneuvers based upon on-board intelligence, but without a COP resident on the aircraft, the same limitations as those in MITL flight apply.

Section 4.0
REQUIREMENTS

4.1 FUNCTIONAL DECOMPOSITION

Reference material from Access5 and from the FAA's Regulatory and Guidance Library provided significant input to the Contingency Management requirements development process. That information, combined with experience of some UAS manufacturers gave excellent insight into formation of the requirements.

4.2 ANALYSIS OF ASSUMPTIONS AND REQUIREMENTS IN CONOPS AND FRD

The Access 5 CONOPS (Concept of Operations) and FRD (Functional Requirements Document) were analyzed and will be updated based on that analysis and on conclusions/ requirements developed by the CM Work Package and by other activities.

4.3 SYNTHESIS OF REQUIREMENTS

4.3.1 Functional Requirements at the UAS System Level

As a result of analyzing the requirements from the CONOPS and the FRD (Functional Requirements Document) and evaluating Category breakdown of the current state of UAS's, and real events, the recommended system level functional requirements are listed below. Rationale and background information is also furnished.

4.3.1.1 MANAGE CONTINGENCIES

The UAS System shall be capable of performing contingency management to reduce the likelihood of loss-of-life or damage to personal property at a level of safety equivalent to manned aircraft.

Rationale and Background:

Contingencies include failures of avionics and other equipment within the UAS, loss of communications both internal and external to the UAS, and failure of pilot or operators to respond to critical events with the UAS. Contingency management (CM) involves evaluating an off-normal event, deciding on the proper course of action (plan) and successfully executing the mitigation plan.

4.3.1.1.1 Predictability

The Air Vehicle Element shall operate safely and predictably while performing emergency procedures.

Rationale and Background:

Equivalent Level of Safety

4.3.1.1.2 Continuous Pilot Control

In the presence of failures and abnormal events that degrade continuous and full time pilot control of the UAS, the Contingency Management System shall provide related means to reduce the likelihood of loss-of-life or damage to personal property.

Rationale and Background:

a. If the pilot is not able to send commands to the UAS because of a break in the command chain, the UAS must still operate in a safe and predictable manner.

b. Refer to Appendix A (Rationale and Background for Requirements 4.3.1.1.2).

4.3.1.1.3 Situational Awareness

In the presence of failures and abnormal events that degrade SA (Situational Awareness) of the UAS, Contingency Management shall provide related means to mitigate and circumvent in order to reduce the likelihood of loss-of-life or damage to personal property.

Rationale and Background:

a. Because the UAS pilot is physically located outside of the aircraft, it is easy to lose situational awareness with a break in the UAS health and status information chain.

b. Refer to Appendix B (Rationale and Background for Requirements 4.3.1.1.3) for additional details on this requirement and potential methods of mitigation.

4.3.1.1.4 Recovery Location

As part of any Contingency Management activity, the UAS System shall always have a recovery location identified in any route it may be flying.

Rationale and Background:

Location is assumed to mean a known location on the earth, which may be a UAS airfield for a normal landing, or an impact point in an unpopulated area.

This requirement may not apply in the event of catastrophic failures, since with catastrophic failures, continued safe flight is not certain.

4.3.1.1.5 Flight Termination

The UAS System shall always have the means to safely terminate flight.

Rationale and Background:

A safely terminated flight is meant to be a flight where the UAS aircraft lands normally at an alternate or emergency airport or impacts a predictable point that has been verified as not having people present.

Appendix A

Rationale and Background for Requirement 4.3.1.1.2 (*In the presence of failures and abnormal events that degrade pilot control of the UAS, the Contingency Management System shall provide related means to reduce the likelihood of loss-of-life or damage to personal property.)*

In this requirement, it is assumed that the pilot is not able to command the aircraft, is not able to divert, to maneuver clear of traffic, nor is he/she able to modify the flight plan at will. The aircraft may be autonomous or flying on autopilot, and may be following a pre-determined flight plan, but the pilot can not interrupt any parts of that plan.

Control of the aircraft is a term that needs clarification. Control of an aircraft can be interpreted to mean control by the on-board mission computer or an autopilot taking directions from a mission plan. Using the autonomous mode as a means of keeping control of the aircraft has been adequate for some currently operating UAS. Another interpretation of Control of the aircraft is the ability of a MITL (Man-in-the-Loop) at a computer console manipulating controls similar to what is done in manned aircraft. The MITL is able to direct the aircraft at will, giving heading changes, altitude changes etc. from an AVCS and controlling the aircraft in that fashion. This also is an acceptable "way to do it" as a means to control the aircraft.

The MITL requires a functioning command path in order to transfer pilot's intentions to the aircraft. This command path consists of a series of components that comprise a "command chain". The important point is that the command chain is more than a transmitting antenna and a receiving antenna. The command must maneuver through a series of components in the ground station, the satellite, and the aircraft. It must travel from the mouse click or control movement, to the flight control surfaces of the aircraft.

If the pilot is not able to send commands to the aircraft because of a break in the command chain, alternate means of controlling the aircraft will be required.

The ability of a UAS pilot to have access to his aircraft's flight controls is unlikely to be 100% assured. In manned aircraft, the pilot's intentions are transmitted to the flight surfaces using a command chain that has reliability figures in the 1 minus 10^{-10} region. This high reliability is easy to understand with quad redundant flight control systems in modern airliners, or more simply, with the cables, pulleys, and pushrods found in the Cessna 172. Figure A-1 illustrates how the command chain works in a manned aircraft compared to a UAS.

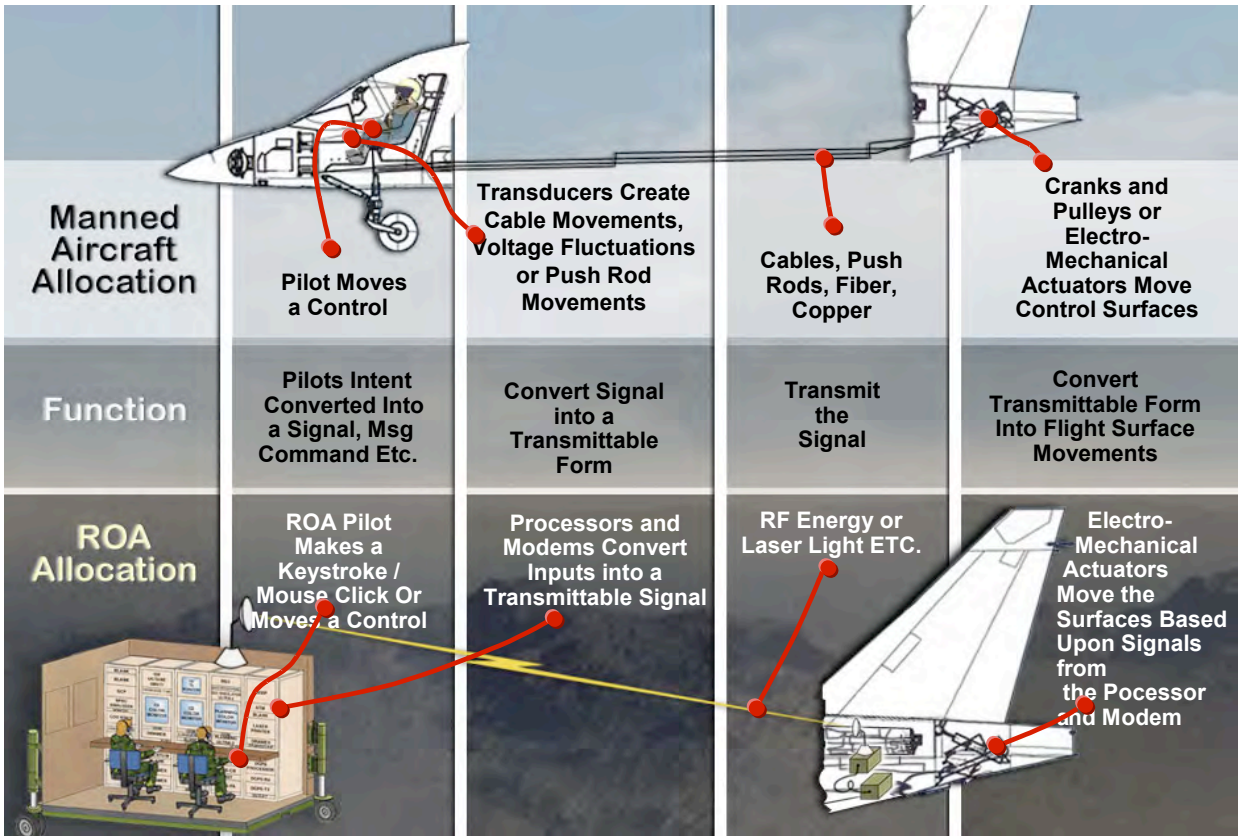


Figure A-1. Unmanned Aircraft Systems Need a High Reliability Command Chain in Order to be Equivalent to Manned Aircraft in Regards to the UAS Pilot's Ability to Send Commands to the Aircraft.

Many things can go wrong with the command chain of a UAS. The consequence of a lost command chain is loss of ability of the UAS pilot to maneuver his/her aircraft.

A break in the UAS command chain does not meet the definition of the traditional lost communications situation. The lost command chain is basically a lost ability to maneuver the aircraft. That is not a lost comm situation. A lost comm situation is defined in the AIM as "Loss of the ability to talk by radio". In functional terms, it means that ATC and the UAS pilot are not able to talk to each other.

In emergencies there are telephones. The UAS pilot can always talk to the supervisor in the ATC agency if necessary. When a flight plan is filed with the FAA in compliance with the COA, a phone number is always placed in the remarks so the FAA is able to call the UAS pilot when normal voice communication fails. It has been used in the Global Hawk community a number of times. This means that the controller can still talk to the pilot, in an emergency. But, even with all of the shortcomings of the workarounds, it's no longer a lost comms situation as soon as the ATC controller and the UAS pilot can again talk to each other, for example, over the telephone.

Does that mean everything is fine as long as the UAS pilot is again able to converse with the ATC controller? Not necessarily, not if the pilot is still not able to send commands to the aircraft. With loss of the command chain, it's a whole different story, it's not a lost comms situation at all.

Is the inability of the UAS pilot to command an aircraft a serious problem? Industry consensus will certainly say it is OK if the pilot on the ground cannot send commands to the

aircraft for short period of time, such as with antenna blockage. Granted, any UAS will experience periods of not being able to be interrupted, and that is acceptable as long as the interruption is related to something other than failures of the data link system. A good example of loss of link is when the satellite has periods of unavailability such as wing blocking during a turn. Procedures are normally in place to mitigate such an anomaly. When that happens, it will be necessary for the aircraft to fly a preprogrammed maneuver or to re-configure itself until the data link is re-established.

When a data link failure is encountered, by definition, the data link is simply not available, and the assumption is that the back-up links are also not available. If the data link is not re-established, the UAS will have to continue on auto-pilot to a particular destination. Now if it cannot continue a safe flight, then it will have to have pre-established abort procedures or abort routes. Most significant is the requirement for the aircraft to execute a safe recovery on its own.

The pilot has continuous contact with the FAA controller or the supervisor through any means available, so loss of the links is not a classic lost comm situation.

Appendix B

Rationale and Background for Requirement 4.3.1.1.3 (*In the presence of failures and abnormal events that degrade SA (Situational Awareness) of the UAS, Contingency Management shall provide related means to mitigate and circumvent in order to reduce the likelihood of loss-of-life or damage to personal property).*

This requires the pilot to use any resource available to re-gain Situational Awareness of his aircraft.

The pilot may or may not experience lost communications with the ATC controller, which would be a different from the situation described here. In the case at hand, the pilot is unable to receive status or send commands to it concerning the aircraft.

Situational Awareness is assumed to include intentions of the aircraft.

Technologies and processes that may be available to provide health/status/intentions to the UAS pilot or to ATC in event of loss of C2 data link are listed below. This list discusses the most promising concepts for development into practical and affordable solutions

Six mitigation measures have been evaluated to regain Situational Awareness after the UAS' health and status feedback chain (return chain) has been interrupted. As was previously discussed for the command chain, the return chain is also vulnerable to interruptions and failures, in most part caused by the same incident that caused the command chain failure.

1. Alternative Data Link – The probability that a UAS would be unable to communicate over any of the C2 data links because of a data link failure is highly remote. Most UAS have multiple LOS and BLOS links that do not have common components susceptible to a single failure. The most likely result in the event of a failed communication link is that a different communication path would need to be selected. The following analysis shows the many different communication paths that could be used to back-up the primary C2 data link.

   The selection of communication technologies may be prioritized using the following parameters:

   a. Availability and Reliability of the Comm
   b. Capacity Bandwidth
   c. Coverage
   d. Access and Control
   e. Interoperability
   f. Affordability
   g. Flexibility
   h. Protection/Security
   i. Latency
   j. Quality of Service
   k. Alternate Communication methods

2. Transponder – FAA regulations require that all aircraft, manned or unmanned (UAS), military or civilian, flying at an altitude of 10,000 feet or higher in U.S. controlled airspace, must be equipped with an operating transponder system capable of automatic altitude reporting.

Modern transponder is a two-channel system, with one frequency (1030 megahertz) used for the interrogating signals and another (1090 megahertz) for the reply. The system is further broken down into four modes of operation, two for both military and civilian aircraft and two strictly for military use.

Each mode of operation elicits a specific type of information from the aircraft that is being challenged. Mode 1, which has 64 reply codes, is used in military air traffic control to determine what type of aircraft is answering or what type of mission it is on.

Mode 2, also only for military use, requests the "tail number" that identifies a particular aircraft. There are 4096 possible reply codes in this mode.

Mode 3/A is the standard air traffic control mode. It is used internationally, in conjunction with the automatic altitude reporting mode (Mode C), to provide positive control of all aircraft flying under instrument flight rules. Such aircraft are assigned unique mode3/A codes by the airport departure controller. General aviation aircraft flying under visual flight rules are not under constant positive control unless it is requested and granted, otherwise such aircraft use a common Mode 3/A code of 1200. In emergencies manned and UASs could use a 77xx code indicating the aircraft has some kind of emergency. In either case, the code number is entered into the transponder control unit. For UASs the transponder code can be automatically updated to reflect the UAS flight status.

Altitude information is provided to the transponder by the aircraft's air data computer in increments of 100 feet. When interrogated in Mode C, the transponder automatically replies with the aircraft altitude. FAA ground interrogators normally interlace modes by alternately sending Mode 3/A and Mode C challenges thus receiving continuous identity and altitude data from the controlled aircraft.

The current air traffic control system is labor intensive for both ground controllers and flight crews and relies heavily on two-way voice communications for the transfer of routine data. As air traffic densities increase, the situation becomes more severe.

To reverse this trend, the FAA has authorized the development of a new system designated Mode S to be implemented for commercial carriers. The system is also being deployed in regions of Europe. The system uses the standard TRANSPONDER frequencies of 1030 and 1090 megahertz, but both the challenge and reply formats are more complexly coded than in the current beacon system. In particular, each aircraft will be assigned a permanent Mode S address, which will share with no other (more than 16 million addresses will be available). Upon the aircraft's entrance into a Mode S control zone, the address will be automatically elicited by the ground control station and entered into a central computer. Thereafter, the aircraft can be uniquely addressed, thus greatly reducing system self-interference. The reply message will also contain the aircraft address, altitude and other selected data that could be used to evaluate the health and status of an UAS in a contingency management condition.

The Mode S system is designed to be compatible with the current air traffic control beacon system, so that the Mode S equipped aircraft can continue to operate in non-Mode S controlled airspace. This will allow the system to be installed in an evolutionary manner. The system also incorporates a number of preplanned growth features that will lead to a highly automated air traffic control system including onboard collision avoidance equipment. The growth features could include the ability to recognize UAS contingency broadcasts. As a general statement concerning the

TRANSPONDER as a back-up tool for re-gaining SA for the UAS pilot, significant changes to the standard catalog of available codes would have to be accepted by the FAA. Codes could be used for catastrophic failures, comm failures, (data link and voice), and other categories to be determined. One limitation is that the aircraft's intentions would not normally be available unless the UAS suppliers made that information available to the TRANSPONDER system, then the code numbers would increase dramatically.

3. ADS-B - Standards for the Automatic Dependent Surveillance - Broadcast (ADS-B) system are currently being developed jointly by the FAA and industry. The ADS-B concept is as follows: UAS aircraft will broadcast a message on a regular basis, which includes it's position (such as latitude, longitude and altitude), velocity, and possibly other information. Other Non-UAS aircraft or systems can receive this information for use in a wide variety of applications. Current surveillance systems must measure vehicle position, while ADS-B based systems will simply receive accurate position reports broadcast by the UAS vehicles.

   As an example, consider an air-traffic control radar. The radar measures the range and bearing of an aircraft. The bearing is measured by the position of the rotating radar antenna when it receives a reply to its interrogation from the aircraft, and the range by the time it takes for the radar to receive the reply. The beam of the antenna gets wider as the aircraft get farther from the antenna, thus making the measured position information less accurate. An ADS-B based system, on the other hand, would listen for position reports broadcast by the aircraft. These position reports are based on accurate navigation systems, such as satellite navigation systems (e.g. GPS). The accuracy of the system is now determined by the accuracy of the navigation system, not measurement errors. The accuracy is unaffected by the range to the aircraft. With the radar, detecting aircraft velocity changes requires tracking the received data. Changes can only be detected over a period of several position updates. With ADS-B, velocity changes are broadcast almost instantaneously as part of the State Vector report. These improvements in surveillance accuracy can be used to support the UAS in a contingency management situation. This capability is under development by the FAA to support a wide variety of applications and increase airport and airspace capacity while also improving safety.

4. Voice Broadcast- Voice Synthesis could be used in conjunction with a non-digital data link to broadcast the intentions and health of the UAS through voice communication channels. This assumes that the analog voice radios are still functioning. This option would easily allow ground-based controllers to have at minimum knowledge of the UAS status.

   The UAS's capability to create a synthesized voice is easily achievable within today's technology. The ability to use the synthesized voice and broadcast through an analog radio channel would provide other air vehicle pilots, and airport operators the information to take action if required to allow the UAS to continue with its flight plan. The UASs would most likely use emergency guard frequencies, however, because of an on-board data-base, the aircraft could use frequencies that are normally used for sectors.

5. Radar tracking (Skin paint capability) - The information secured by radar includes the position and velocity of the UAS with respect to the radar unit. Commercial airports are

equipped with radars that warn of obstacles in or approaching their path and give accurate altitude readings. These radars could be used to detect an UAS with a communication failure. The radar would only be able to determine the UAS's position, and not it's status or health, unless the information is compared to the simulated contingency results. Latency and accuracy degrade as distances between the UAS and the radar antenna increase.

The ability to predict through system simulation the UASs intended path coupled with the ability to radar track the UAS enables the pilot to deduce the health and status of the UAS within very limited conditions. But this capability may allow the UAS pilot or the UAS itself to find, diagnose, and fix the on-board problem.

6. System Simulation- All autonomous UAS flight management software is the result of many hours of simulated flight activity. The simulations are used to develop and validate the flight control and flight management software. The simulation process enables the developers to subject the UAS to many different changes in the external factors that can affect the performance of the UAS under normal flight operations. This simulation capability can be extended to cover the operations of the UAS in contingency management operations.

   The system simulation, coupled with information that could be obtained through the ADS-B, or through radar with TRANSPONDER could provide a sufficient operational picture to deduce the intentions and health of the UAS. A typical example would be if all the normal data-link communication capability were lost aboard the UAS, the UAS could broadcast its intentions via the ADS-B system. The ADS-B data would be very limited, but could include the information to allow the UAS pilots to conclude all other UAS systems are operating normally and allow the UAS to continue the mission. The system simulation would then provide the guidance to predict the UAS's intended path. But more importantly should the UAS stray from the system simulation's predicted path then emergency UAS pilot action may be required. This situation would be used to guarantee that an uncontrollable UAS would not enter congested civilian traffic or endanger people on the ground.

Appendix C
Multiple Failures

C-1.0 BACKGROUND

Access5 is a NASA funded program that has the goal of facilitating integration of Unmanned Aircraft System (UAS) into the NAS (National Airspace System). A consortium of UAS industry members and NASA Research Center members who are tasked with formulating requirements and performing simulations and flight tests, results of which will be presented to the FAA. The FAA will use those inputs in forming up policy, procedures, and criteria for certification of UAS's. The ultimate objective is to allow the UAS to file and fly in the NAS with a level of safety equivalent to manned aircraft.

C-2.0 SCOPE

The CM (Contingency Management) WP (Work Package) is part of the Technology IPT (Integrated Product Team). CM is responsible for creating functional requirements that will ultimately be used by industry suppliers who apply for certification of UAS's in the NAS. During FY-05, the CM WP will produce updated CM requirements and will create new requirements in the areas of Mission Planning, in addition to the identification of scenarios for flight test and for Airspace Operations Simulations.

C-3.0 PURPOSE OF THIS APPENDIX

Appendix C discusses the concepts of multiple failures in UASs, and what, if any, requirements may be derived. It includes a review of pertinent definitions, how many aircraft are currently designed, what mitigating actions are used, and how multiple failures could be resolved in future UAS designs.

C-4.0 GENERAL CONCEPTS AND DEFINITIONS CONCERNING FAILURES

To fully understand multiple failures, one must first fully comprehend the definitions of a single failure. Multiple failures will also be discussed in this section. Dual failures, a sub-set of multiple failures, are covered in Section C-5.0

C-4.1 SINGLE FAILURE DISCUSSION

A failure is defined in AC 23.1309 and AC 25.1309 as:

> ***Failure*:** An occurrence that affects the operation of a component, part or element such that it can no longer function as intended. (This includes both loss of function and malfunction). Note: Errors may cause failures but are not considered failures.[1]
>
> ***Failure*:** A loss of function or malfunction of a system or part.[2]
>
> For purposes of this document, a single failure includes all of the consequences and associated propagated failures that it causes. For example, an engine failure that causes a hydraulic system failure would be considered a single failure rather than a dual failure.

[1] Advisory Circular 23.1309-1C *Equipment, Systems, and Installations in Part 23 Airplanes*. March 22, 1999; Pg. 8
[2] Advisory Circular 25.1309-1A S*ystem Design and Analysis*. June 21, 1988; Pg. 4

C-4.1.1 Single Failure Definitions

Single failures come in a multitude of flavors, but four general categories have been identified in MIL-STD-882C as major contributors to the general definition of a failure. Those four categories are:

Single Component Failures: The single component failure is the most common and also get the most attention in safety assessments. The single component failure is also the first thing that comes to mind when a "failure in the system" is declared.

Common Mode Failures: A common mode failure is an event which affects a number of elements otherwise considered to be independent. Common cause failures are similar in that they bypass or invalidate redundancy or independence.

Human Errors: Human errors are failures caused by the human element of the Human System Interface.

Design Features: Design features are the failures that are caused by defects in the design of a system.

C-4.1.2 Probabilities Assigned to Single Failures Using Qualitative Descriptions

Qualitative descriptions of probability conditions provide textual rather than numerical measures, and are therefore less precise.

Probable Failure Conditions: Those Failure conditions anticipated to occur one or more times during the entire operational life of each airplane. They may be determined on the basis of past service experience with similar components in a comparable airplane application.[3]

Improbable Failure Conditions: Failure conditions unlikely to occur in each airplane during its total life but that may occur several times when considering the total operational life of a number of airplanes of this type. Also, those Failure conditions not anticipated to occur to each airplane during its total life but that may occur a few times when considering the total operational life of all airplanes of this type. For quantitative assessments, refer to the probability values shown for Major and Hazardous Failure Conditions in conversion tables readily available in the references [4]

Extremely Improbable Failure Conditions: For commuter category airplanes, Failure Conditions so unlikely that they are not anticipated to occur during the entire operational life of all airplanes of that type. For other classes of airplanes, the likelihood of occurrence may be greater.[5]

C-4.1.3 Severity Assigned to Single Failures

Minor Failure Condition: Failure conditions which would not significantly reduce airplane safety, and which would involve crew actions that are well within their capabilities.[6]

Major Failure Conditions: Failure conditions that would reduce the capability of the airplane or the ability of the crew to cope with adverse operating conditions to the extent that there would be a significant reduction in safety margins or functional capabilities; a significant

---

[3] Military Standard 882C Military Standard System Safety Program Requirements. 19 January 1993; Pg. 10

[4] Advisory Circular 23.1309-1C Equipment, Systems, and Installations in Part 23 Airplanes. March 22, 1999; Pg. 16

[5] Advisory Circular 23.1309-1C Equipment, Systems, and Installations in Part 23 Airplanes. March 22, 1999; Pg. 9

[6] Advisory Circular 23.1309-1C Equipment, Systems, and Installations in Part 23 Airplanes. March 22, 1999; Pg. 8

increase in crew workload or in conditions impairing crew efficiency; or a discomfort to the flight crew or physical distress to passengers or cabin crew, possible including injuries.[7]

Catastrophic Failure Condition: Failure Conditions that are expected to result in multiple fatalities of the occupants, or incapacitation or fatal injury to a flight crewmember normally with the loss of the airplane. Note: (1) The phrase "are expected to result" is not intended to require 100 percent certainty that the effects will always be catastrophic. Conversely, just because the effects of a given failure, or combination of failures, could conceivably be catastrophic in extreme circumstances, it is not intended to imply that the failure condition will necessarily be considered catastrophic. (2) The term "Catastrophic" was defined in previous versions of the rule and the advisory material as a Failure Condition that would prevent continued safe flight and landing.[8]

C-4.1.4 Mitigation of Single Failures

C-4.1.4.1 Unacceptable Failure Condition Definition From MIL-STD-882C. Most military systems require that no single point failure will result in a catastrophic event.

MIL-STD-882C identifies single failures that can cause a catastrophic or critical severity mishap, as an unacceptable condition that needs to be mitigated to reduce risk to an acceptable level. Figure C-4.1.4-1 gives a representation of how single point failures are depicted in MIL-TD-882C.

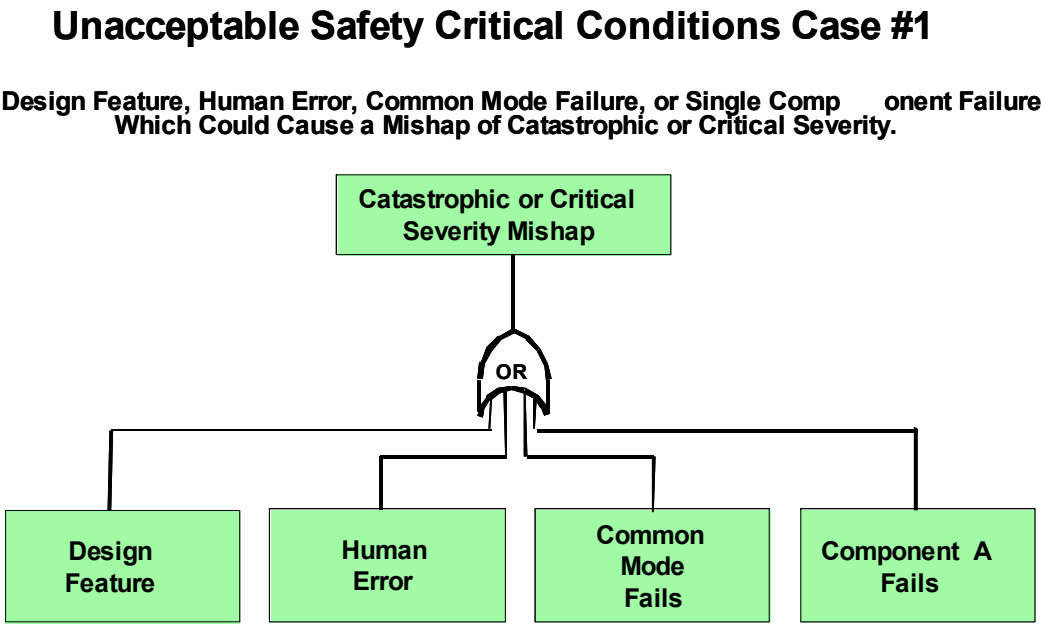


Figure C-4.1.4-1. If Any One of the Four Single Point Failures Could Cause a Catastrophic or Critical Severity Mishap, Positive Action is Required

C-4.1.4.2 Unacceptable Failure Condition Definition From FAR Part 25. The Part 25 airworthiness standards are based on, and incorporate, the objectives, and principles or techniques, of the fail-safe design concept, which considers the effects of failures and combinations of failures in defining a safe design.

[7] Advisory Circular 23.1309-1C Equipment, Systems, and Installations in Part 23 Airplanes. March 22, 1999; Pg. 8
[8] Advisory Circular 23.1309-1C Equipment, Systems, and Installations in Part 23 Airplanes. March 22, 1999; Pg. 9

a. The following basic objectives pertaining to single failures apply:

In any system or subsystem, the failure of any single element, component, or connection during any one flight (brake release through ground deceleration to stop) should be assumed, regardless of its probability. Such single failures should not prevent continued safe flight and landing, or significantly reduce the capability of the airplane or the ability of the crew to cope with the resulting failure conditions [9]

C-4.1.4.3 Unacceptable Failure Condition Positive Actions From AC 25.1309. The fail-safe design concept uses the following design principles or techniques in order to ensure a safe design. The use of only one of these principles or techniques is seldom adequate. A combination of two or more is usually needed to provide a fail-safe design; i.e., to ensure that major failure conditions are improbable and that catastrophic failure conditions are extremely improbable.

(1) Designed Integrity and Quality including Life Limits, to ensure intended functions and prevent failures.

(2) Redundancy or backup systems to enable continued function after any single (or defined number of) failures(s); e.g., two or more engines, hydraulic systems, flight control systems, etc.

(3) Isolation of Systems, components, and Elements so that the failure of one does not cause the failure of another. Isolation is also termed independence.

(4) Proven Reliability so that multiple, independent failures are unlikely to occur during the same flight.

(5) Failure Warning or Indication to provide detection.

(6) Flight crew Procedures for use after failure detection, to enable continued safe flight and landing, by specifying crew corrective action.

(7) Checkability: the capability to check a component's condition.

(8) Designed Failure Effect Limits, including the capability to sustain damage, to limit the safety impact or effects of a failure.

(9) Designed Failure Path to control and direct the effects of a failure in a way that limits its safety impact.

(10) Margins or Factors of Safety to allow for any undefined or unforeseeable adverse conditions.

(11) Error-Tolerance that considers adverse effects of foreseeable errors during the airplane's design, test, manufacture, operation, and maintenance.[10]

The positive actions are depicted in Figure C-4.1.4-2 below for a typical single point failure.

[9] Advisory Circular 25.1309-1A S*ystem Design and Analysis*. June 21, 1988; Pg. 4

[10] Advisory Circular 25.1309-1A S*ystem Design and Analysis*. June 21, 1988; Pg.2-3

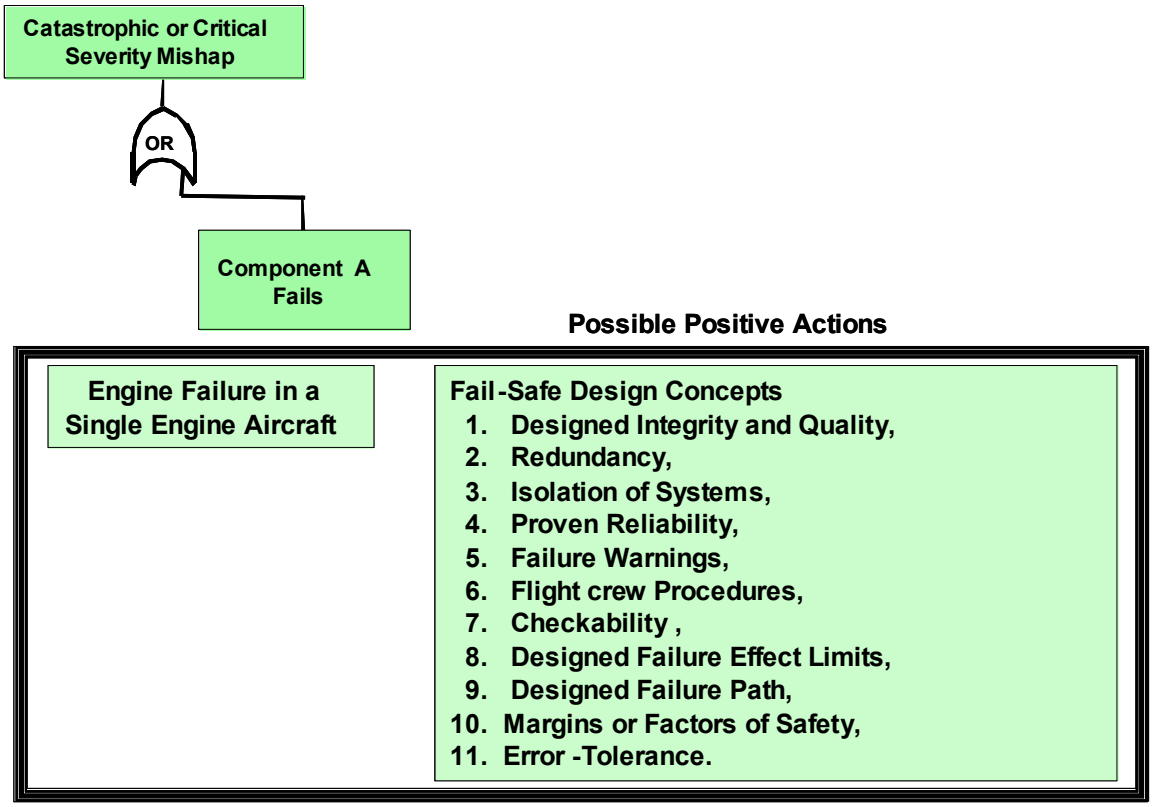


Figure C-4.1.4-2. With a single component failure that causes a catastrophic or critical severity mishap, positive actions are required IAW MIL-STD-882C.

C-4.1.5 Specific Example of a Single Failure That is Unique to the UAS

Loss of the function "Control the Aircraft Remotely" is a failure that is unique to the UAS. In manned aircraft, the normal way commands are sent to the aircraft is for the pilot to enter the appropriate movements to the control yoke or to the autopilot and the aircraft responds. With the UAS, those commands are sent through a data link and the associated processors and modems to indicate to the aircraft that a movement is required in the control surfaces.

In a manned aircraft, entry of the command is assured by a simple and reliable process. With the UAS however, the data links and associated components in the chain are more complex, and the path is more complicated, having to rely on components that are remote, and not under the complete control of the pilot.

The actual medium all by itself is subject to various hazardous, including component failure and security breaches.

Components belonging to the AVCS and to the Aircraft are also subject to the same vulnerabilities that the medium has to endure. The critical components in the AVCS element and in the aircraft element involved in the function "control the aircraft remotely" are serial in nature and therefore need to be adequately analyzed and accounted for through a series of safety assessments. The reliability in the two elements can only be defined when those assessments have been performed and the mitigation actions have been designed in.

To characterize the reliability of the command path all single point failures in the entire path must be identified and mitigated.

The command path in the UAS could be safety critical depending upon how the vehicle is designed. Safety Critical is defined as:

> ***SAFETY CRITICAL****: A term applied to a condition, event, operation, process or item of whose proper recognition, control, performance or tolerance is essential to safe system operation or use; e.g., safety critical function, safety critical path, safety critical component.*[11]

Thus, it can be determined from the discussion that when the function "control the aircraft remotely" is safety critical, failure mitigation strategies will be required to insure reliability levels for the entire command path will be similar to those found in manned aircraft.

C-4.2 MULTIPLE FAILURE DISCUSSION

C-4.2.1 Relationship Between Single Failures and Multiple Failures

The definition of multiple failures assumes both of the failures are detected at the same time. If one of the failures is not detected, then a single failure condition exists. Multiple failure is defined as:

> ***MULTIPLE FAILURE:*** *The presence of more than one of the previously defined single failures at the same time during the same flight. Each of the simultaneous failures must be independent, non-related, and must not have a common cause.*

An engine failure may affect one or more subsystems and therefore cause a failure in one or more of those subsystems. For example, engine failure and hydraulics failure sound like two separate failures. The single failure propagates or cascades down to the lower level sub-system, and gives the appearance that these are multiple failures.

The difference between multiple single independent failures, and multiple failures caused by a single event is difficult to assess, and delays can occur while attempting to identify the root cause of the failure.

Repeat of a single failure during the flight, after the previous occurrence has been corrected, can not be considered to be a multiple failure for purposes of this analysis.

A failure of a completely different system that is independent of the first failure, after the first failure has been corrected, will be treated as a single failure. If a common cause or a common mode has been identified then it definitely is a single failure.

Multiple failures are those that exist simultaneously while the aircraft is on a mission. This includes taxi, takeoff, and landing rollout.

From the pilot's perspective, dual failures that involve the Command and Control (C2) function are the most difficult to deal with. With UAS's, multiple failures that do not involve the C2 function can be mitigated in the same manner that they are mitigated in manned aircraft, i.e., the pilot is able to apply corrective action as specified by the manufacturer's design. However, when the dual failure involves the C2 function, the order of the failures has significant impact. When the C2 function fails first, the pilot is not able to detect a subsequent failure, and he will not be able to apply the corrective actions to that subsequent failure. Conversely, when the first failure is a different single point failure, then there are some options available until the C2 function fails.

---

[11] Military Standard 882C *Military Standard System Safety Program Requirements*. 19 January 1993; Pg. 6

C-4.2.2 Latent Failures

Latent failures are defined as:

> ***LATENT FAILURE:*** *A failure is latent until it is made known to the flight crew or maintenance personnel. A significant latent failure is one that would, in combination with one or more specific failures or events, result in a hazardous or Catastrophic Failure Condition.*[12]

The subject of latent failures will not be analyzed at this time. Unless the flight crew knows the failure is there, he is not able to troubleshoot and apply the corrective action. When an independent failure occurs, it will be considered a single failure, and corrective action will be required to mitigate the problem. When and if an additional failure occur and it is a latent failure, there is no reason to take other action except that which is needed to correct the earlier known failure.

C-5.0 ANALYSIS OF DUAL FAILURES

Dual failures are a sub-set of the multiple failures mentioned above. Two independent references contain definitions that help to illustrate toe concepts of dual failure. Neither of the references should be assumed to be directive in nature.

C-5.1 DUAL FAILURES DEFINED IN PART 25

The Part 25 airworthiness standards discuss subsequent failures in addition to single failures. Subsequent failures are defined as:

> ***SUBSEQUENT FAILURES****: Subsequent failures during the same flight, whether detected or latent, and combinations thereof, should also be assumed, unless their joint probability with the first failure is shown to be extremely improbable.*[13]

For purposes of this document, subsequent failures are synonymous with dual failures.

C-5.2 DUAL FAILURES DEFINED IN MIL-STD-882C

The following safety critical conditions are considered unacceptable as described in MIL-STD-882C. Positive action and implementation verification is required to reduce the risk to an acceptable level.

> *Dual independent component failures, dual human errors, or a combination of a component failure and a human error involving safety critical command and control functions, which could cause a mishap of catastrophic or critical severity.*[14]

Figure C-5.2-1 graphically shows the structure of the dual failure definition from MIL-STD-882C.

---

[12] Advisory Circular 23.1309-1C *Equipment, Systems, and Installations in Part 23 Airplanes*. March 22, 1999; Pg. 9

[13] Advisory Circular 25.1309-1A S*ystem Design and Analysis*. June 21, 1988; Pg. 2

[14] Military Standard 882C *Military Standard System Safety Program Requirements*. 19 January 1993; Pg. 110

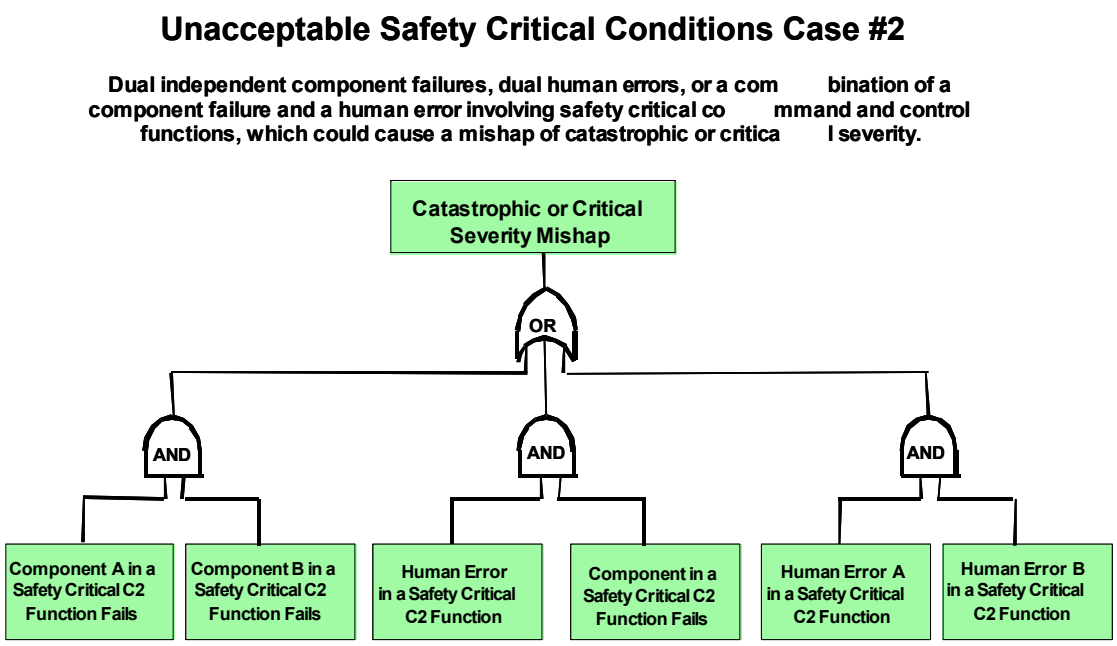


Figure C-5.2-1. Dual Failures

Figure C-5.2-2 and Figure C-5.2-3 show examples of how the above depiction of dual failures can occur in a UAS System.

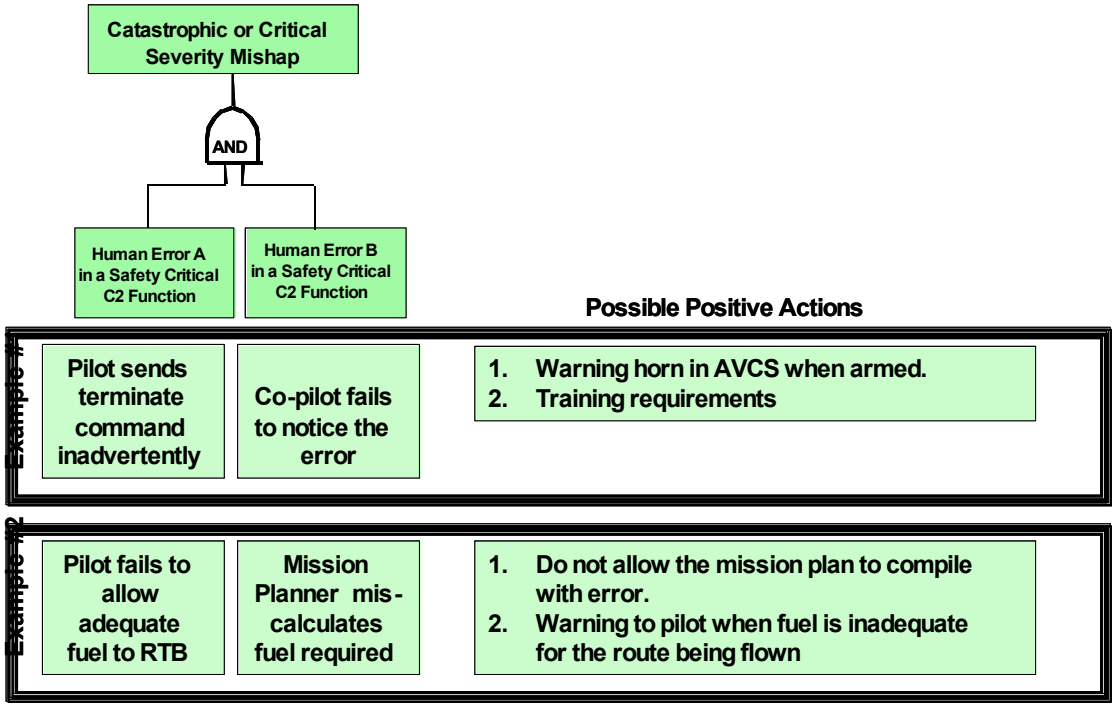


Figure C-5.2-2. Example of Dual Human Errors in a Safety Critical C^2 Function

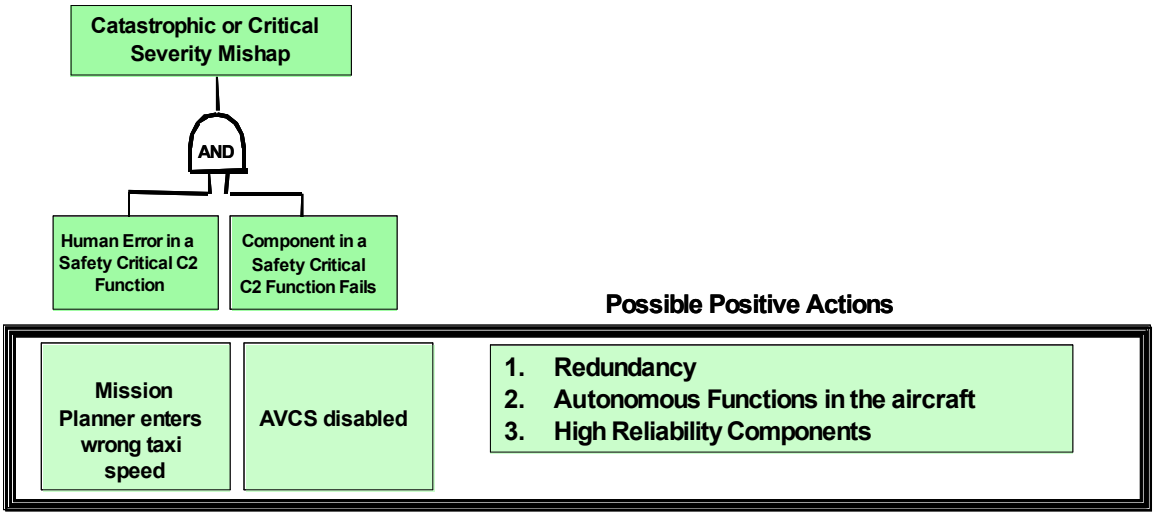


Figure C-5.2-3. Example of Component Failure and a Human Error in a Safety Critical C² Function

C-5.3 MITIGATION OF DUAL FAILURE CONDITIONS

Dual failures (simultaneous, independent, single point failures) are addressed in two separate references (FAR Part 25 MIL-STD-882C) with a different approach for each.

C-5.3.1 FAR Part 25

Part 25 uses a probabilistic approach; the supplier is expected to account for dual failures only if their joint probability of occurrence is extremely improbable. That probability value is $1x10^{-9}$ (Extremely Improbable-failure conditions are those having a probability on the order of $1x10^{-9}$ or less.)[15]

C-5.3.2 MIL-STD-882C

MIL-STD-882C states the supplier is expected to account for dual failures only if they occur in safety critical command and control functions. MIL-STD-882C describes dual failures as an unacceptable condition, but only if they occur somewhere in the Command and Control (C^2) function.

The concepts described in MIL-STD-882C may offer a more realistic approach then AC 25 for mitigation of independent dual failures in Unmanned Aircraft Systems. Part 25 aircraft certification standards focus on multiple casualties as probable in catastrophic mishaps. Depending on the capability of the UAS, it may heavily depend on the C2 data Link, which is a significant component in the Command and Control function. For that reason it is recommended that the standard and requirements for UASs adopt the concepts of MIL-STD-882C concerning dual failures.

C-5.4 THE ROLE OF SAFETY ASSESSMENTS

Early decisions in product development cycles have impact on the types and extent of safety assessments. It is important to establish definitive system safety program requirements for the procurement or development of systems. The requirements must be set forth clearly in the appropriate system specifications and contractual documents.

[15] Advisory Circular 25.1309-1A S*ystem Design and Analysis*. June 21, 1988; Pg. 15

Safety assessments are a common tool used in development of highly complex systems. UAS's can also the subject of these assessments. Advisory Circular (AC) 25.1309 (b) and (d) specify required safety levels in qualitative terms, and require that a safety assessment be made. Various assessment techniques have been developed to assist in determining that a logical and acceptable inverse relationship exists between the probability and the severity of each failure condition. These techniques include the use of service experience data of similar, previously approved systems, and thorough qualitative analysis.[16]

In addition, difficulties had been experienced in assessing the acceptability of some designs, especially those of systems, or parts of systems, that are complex, that have a high degree of integration, that use new technology or new or different applications of conventions, technology or that perform safety-critical functions. These difficulties led to the selective use of rational analyses to estimate quantitative, probabilistic and the development of related criteria based on historical data of accidents and hazardous incidents caused or contributed to by failures. These criteria, expressed as numerical probability ranges associated with the terms used in AC 25.1309 (b) became commonly-accepted for evaluating the quantitative analyses that are often used in such cases to support experienced engineering and operational judgment and to supplement qualitative analyses and tests.[17]

Common Cause analysis deals with failures in one subsystem that have an affect on other subsystems. One of the major objectives of common cause analysis is finding single faults in redundant systems that will affect both systems.[18]

C-6.0 CURRENT PHILOSOPHY OF FIELDED SYSTEMS

C-6.1 GLOBAL HAWK

(No information available)

C-6.2 PREDATOR

(No information available)

C-6.3 HELIOS

(No information available)

C-6.4 PERSEUS

Perseus has Fault Tolerant Control (FTC) software installed which enables the aircraft to handle a single failure of a sensor or actuator without direct flight crew input. If FTC recognizes that a flight sensor or actuator has failed, it can issue a command telling the aircraft to ignore that sensor; i.e., assume it is reading a benign value. The value down linked to the ground control system (GCS) is displayed on the Heads-Up Display (HUD) and flight crew displays is the failed value which will no longer be passed to the autopilot.

If a sensor or actuator is determined to have failed the FTC system will use a redundant sensor and indicate the failure on the MacCopilot warnings page. The aircraft will be controllable throughout the normal envelope, but a decrease in control effectiveness may result with actuator failures.

---

[16] Advisory Circular 23.1309-1C *Equipment, Systems, and Installations in Part 23 Airplanes*. March 22, 1999; Pg. 2

[17] Advisory Circular 23.1309-1C *Equipment, Systems, and Installations in Part 23 Airplanes*. March 22, 1999; Pg. 2

[18] Advisory Circular 23.1309-1C *Equipment, Systems, and Installations in Part 23 Airplanes*. March 22, 1999; Pg. 2

C-6.4.1 Single Failures

C-6.4.1.1 Single Component Failures

Engine

Perseus is a single engine aircraft. In the event of an engine failure the aircraft will experience drastic performance losses. All attempts are made to return the aircraft to the air field launched from. If unable to return to base, an attempt will be made to ditch the aircraft as safely as possible.

The Perseus B follow on will incorporate the ability to attempt re-starting the engine while in flight. Only two attempts will be available with a stalled/ seized engine. After two attempts the auxiliary battery voltage will have dropped below the level capable of engaging the starter unit.

Propellers

Perseus is a single propeller aircraft. Any significant damage to the propeller will reduce thrust characteristics drastically. The aircraft will show an increase in RPM, due to the diminished effectiveness of the propeller.

The propeller hub on Perseus incorporates an accelerometer to measure its vibration. In the event of excessive vibration, an auto feather mechanism will prevent damage to the empennage by killing the engine and feathering the propeller.

Throttle

The throttle servo is a single servo with no backup modes.

Ground Control System (GCS)/ Ground Data Terminal (GDT)

The GCS/GDT has redundant data links to reduce the possibility of a complete loss of link emergency. A single point failure that is inherent in the GDT is the directional antenna rotor. This rotor enables the GDT to track the UAV through out its mission. In the event that the rotor assembly should fail there are two options that may be performed. The first option is to manually rotate the antenna, using the reported single strength to track the air vehicle. A second possible solution is to switch to the omni antenna. This second option is only available within a limited range from the airfield.

C-6.4.1.2 Common Mode Failures. A common mode failure may not be recognized if the data link failure is the first failure to occur. All subsequent failures will go un-recognized due to the lack of down linked data reports. One common mode failure that is accepted is the generators and the engine. In the event of an engine failure, the generators will also fail. The generator failure is acceptable due to the insignificance of the generators failing in relation to the engine failure.

C-6.4.1.3 Human Errors. Human errors are reduced through extensive training of pilots prior to certification as a qualified pilot. Personnel selected to operate Perseus have demonstrated high levels of system knowledge. Simulator training is performed to reinforce this knowledge. While using the simulator all aspects of flight, from normal operations to emergency procedures are evaluated.

Pilot proficiency is reviewed to ensure that all personnel involved with flight operations have performed both simulated and actual flights. Personnel complete regular recurrent training to compliment their high level of system knowledge.

Personnel are typically cross trained to be able to perform two crew functions; i.e., pilot, flight engineer, flight director / mission commander. By possessing knowledge of crew member's positions, errant commands can be evaluated for accuracy and corrected by other crew members. Flight crew members are also trained in crew resource management. This maximizes the effectiveness of all personnel during normal operations and in the case of emergency procedures.

C-6.4.1.4 Design Features. The GCS of Perseus incorporates both visual and audible warnings to alert the pilot of failures as they occur. These warnings are the first link in a chain of events that are initiated to control an emergency situation.

Embedded in the flight control software of Perseus are limitation values that will not allow the aircraft to be commanded into an unsafe flight mode. These limitations are based on known safe operating characteristics.

The electrical system is designed to prevent stray voltage from causing damage to the attached components. Dual generators are monitored for voltage output. If the voltage output of a generator is out of regulated limitations the output is shunted to ground. To further protect the attached circuitry, diodes are placed in line to stop errant current from flowing back into the flight control system. The diodes serve to allow voltage to travel only in one direction. By controlling the path of the voltage the possibility of multiple components failing is virtually eliminated.

C-6.4.2 Dual Failures

C-6.4.2.1 Dual Independent Component Failures. UAV emergencies are handled using hierarchal decision scheme. If two components fail at the same time the more critical emergency is addressed and appropriate actions taken. All emergencies are handled with aviate, navigate, communicate as the backbone for the decision making process. If the pilot experiences a downlink failure, he may not be aware that an engine fail has also occurred due to the lost link characteristics.

C-6.4.2.2 Dual Human Errors. The likelihood of dual human errors is reduced by extensive training, adherence to standard operating procedures, established checklists, crew coordination, and functional cross checks. To mitigate this circumstance a standardized HUD has been installed, guarded switches, and enabled software checks of switch positions to query the accuracy of commands, and modified flight control software to request a confirmation to validate inputs prior to acceptance.

C-6.4.2.3 A Combination of One Independent Component Failure and One Human Error. Extensive crew training, adherence to standard operating procedures, established checklists, crew coordination, and functional cross checks significantly reduce the possibilities of a combination of this nature occurring. This circumstance can extenuate lesser emergencies into catastrophic results. Misdiagnoses of initial malfunction criteria will quickly compound the emergency. The only combative steps to be taken to avoid this situation are training of crew members through simulated emergency practice. Full system knowledge and experience with degrading component characteristics will alleviate failures of this nature.

C-7.0 GUIDELINES CONCERNING DUAL FAILURES

C-7.1 GUIDELINE

IF THE COMMAND AND CONTROL FUNCTION IN THE UAS IS FLIGHT SAFETY CRITICAL, THEN THERE SHOULD BE NO SINGLE POINT FAILURE.

C-7.2 AMPLIFYING INFORMATION CONCERNING THE GUIDELINE

This guideline covers the dual failure that involves the command and control function as one of the two failures. The most troublesome dual failure in the UAS industry is when one of the two failures involves the command and control function.

This guideline applies to any UAS in general without regard to other failures on the same flight, but if the guideline is adopted as a requirement, dual failure mitigation will be easier to manage by the pilot.

Bibliography

1. Advisory Circular 23.1309-1C *Equipment, Systems, and Installations in Part 23 Airplanes*. March 22, 1999

2. Advisory Circular 25.1309-1A S*ystem Design and Analysis*. June 21, 1988

3. Military Standard 882C *Military Standard System Safety Program Requirements*. 19 January 1993.

Appendix D
ONBOARD SYSTEM FAILURES, CCA FAILURES, AND ABNORMAL/EMERGENCY TERMINATION OF FLIGHT GUIDELINES

The UAS system should have a means to discriminate between serious failures and those of little consequence to the safe operation of the aircraft.

The primary guideline is to incorporate a vehicle management system capable of immediately responding to system failures. The vehicle management system should minimize the effect of a discrete system failure on other systems and to mitigate aircraft damage or loss. A vehicle management system should combine system wide integrity management software, backup systems and UAS pilot contingency and emergency situation procedures.

The following sections delineate a set of contingency management guidelines for onboard system failures. Communication system failures are not considered in this document since these failures are covered in the parent document (Contingency Management Requirements). At the end of each section, traceability of each set of requirements to the Contingency Management System Level Requirements is cited.

Dual or multiple failures on-board the aircraft are covered in a separate appendix.

D-1 PROPULSION SYSTEM FAILURES

Propulsion System Failures should be mitigated in such a manner that the aircraft will be recoverable and/or will not cause loss of life or damage to property.

1. Under normal engine/propulsion system failures, the vehicle management system should be capable of minimizing adverse impact to other systems.
2. Mechanisms should be in place for an UAS pilot to verify engine out condition.
3. The UAS's vehicle management system should have the capability to terminate the mission and initiate a flight route to the nearest suitable airfield or Return to Base (RTB).
4. UAS pilot workload should be minimized to the extent required for the pilot to intervene with control inputs that minimize the hazard created by the engine-out.
5. In the event a propulsion system failure results in the aircraft being non-recoverable, the vehicle management system should be capable of setting the aircraft down in a pre-designated off-field landing area or the nearest suitable airfield.
6. IFF modes and codes should have the ability to reflect a propulsion system failure.[19] Automatic transition to a propulsion system failure IFF code is recommended.[20]
7. Report propulsion system failure events to ATC immediately following all appropriate mitigating actions. This is a pilot-in-command responsibility by regulation (91.123(c)).
8. ATC may require pre-designated off-field landing areas.

These guidelines can be traced to Contingency Management System Level Requirements 1, 2, 3 and 5.

[19] Several distinct IFF codes for ROA discrete problems and system failures are being considered.
[20] This case assumes the failure is not directly known by the ROA pilot.

D-2 POWER SYSTEM FAILURES

Power System Failures should be mitigated in such a manner that the aircraft will be recoverable and/or will not cause loss of life or damage to property.

1. Power systems should have sufficient capacity to supply flight critical systems adequate power for extended engine out operation.
2. Power or battery systems should have the capability of supporting engine out flight from any mission altitude and profile to an alternate or suitable landing area.
3. Power systems should be sized to manage all flight critical systems during propulsion system failures for a standard sustained time: a time nearly equivalent to the maximum glide range at maximum operational altitude.
4. A backup power system should be available for all flight critical systems.
5. A backup power system should be available for safe termination of flight.

These guidelines can be traced to Contingency Management System Level Requirements 1, 2, 3, 4, 5 and 6.

D-3 FLIGHT CONTROL SYSTEM FAILURES

Flight Control System Failures should be mitigated in such a manner that the aircraft will be recoverable and/or will not cause loss of life or damage to property. Redundant flight control systems coupled with fault tolerant or system wide integrity management software will serve to significantly mitigate flight control system failures.

1. In the event of a primary flight control system failure, the flight control system should have the capability to transfer to a backup flight control mode. Software and hardware backup guidelines should be considered separately.[21]
2. If the UAS experiences total flight control system failure – which includes backup control mode failure – the vehicle management system should have the capability to:
    a. detect flight and mission critical system failures in non-redundant systems and notify the UAS pilot,
    b. when conditions warrant, terminate flight (refer to definition in Sec D-8)
    c. change IFF mode to indicate total flight control system failure[22]
3. In the event of flight control system automated functions failure, the UAS pilot should have the ability to assume command of the UAS from automated flight control system functions.
4. Flight control system primary sensors (AOA, AOS, altimeter, etc.) should have appropriate backup systems to ensure failure mitigation.

These guidelines can be traced to Contingency Management System Level Requirements 1, 2, 3, 4 and 6.

[21] Software certification levels should be considered in defining this requirement.
[22] Several distinct IFF codes for ROA discrete problems and system failures are being considered. This case assumes the failure is not directly known by the ROA pilot.

D-4 NAVIGATION SYSTEM FAILURES

Navigation System Failures should be mitigated in such a manner that the aircraft will be recoverable and/or will not cause loss of life or damage to property.

1. The navigation system should have appropriate backup systems to ensure safe return to base or landing at a suitable auxiliary airfield.
2. In the event of a navigation system failure, the UAS system should have access to other systems to permit an UAS pilot to directly control a safe return to base.

These guidelines can be traced to Contingency Management System Level Requirements 1, 2, 4, 5 and 6.

D-5 SENSOR & PAYLOAD SYSTEM FAILURES

Sensor and Payload System Failures should be mitigated in such a manner that the aircraft will be recoverable and/or will not cause loss of life or damage to property.

Visual sensors are typically used for mission execution, denying or confirming wing ice accumulation, and sometime for weather avoidance.[23]

1. As a guideline, payload systems should utilize power sources separate from flight critical system power sources. Payload systems should be isolated from other vehicle systems to extent required to prevent a propagation effect that causes failures in other aircraft sub-systems, especially flight critical systems, backup systems and non-redundant systems.
2. Payload software should also be isolated from flight critical systems. As a minimum guideline, payload systems should not be used as bus controllers on an UAS critical avionics bus.
3. Payload and sensor systems should have the capability of being immediately shut down or disengaged from power sources at failure initiation via some form of mode control or system integrity management.

These guidelines can be traced to Contingency Management System Level Requirements 1, 2, 3, and 4.

D-6 CCA SYSTEM FAILURES

Cooperative Collision Avoidance (CCA) System Failures should be mitigated in such a manner that the aircraft will be recoverable with a pilot-in-the-loop and/or will not create a collision hazard where none existed. CCA is:

A Cooperative Collision Avoidance (CCA) system failure can potentially be isolated to: a sensor failure, a data link failure, system antenna, or a software failure or anomaly. The data link, in a cooperative collision avoidance system, is the most critical component. Failure of the data link implies failure of the CCA system. As a guideline, the UAS system should change IFF modes to indicate non-cooperative, and, if feasible, to indicate CCA system failure.[24]

As a guideline, non-cooperative collision avoidance system failures should not influence flight critical systems.

---

[23] Some ROA systems utilize color nose cameras to assist aerial vehicle pilots with vehicle flight control. However, instruments comprise the *primary* flight critical system for takeoff and landing.

[24] Several distinct IFF codes for ROA discrete problems and system failures are being considered. This case assumes the failure is not directly known to the ROA pilot.

These guidelines can be traced to Contingency Management System Level Requirements 1, 2, 3, and 4.

D-7 MECHANICAL AND OTHER SYSTEM FAILURES

Mechanical and Other System Failures, not related to flight critical systems, should be mitigated in such a manner that the aircraft will be recoverable and/or will not cause loss of life or damage to property.

Mechanical systems failures are very difficult to mitigate with contingency planning. However, as a guideline, mechanical system failures should be isolated from flight critical systems.

Fault tolerant systems could be employed to mitigate control surface or other structural or mechanical system failures. As a guideline, contingency management for these structural or mechanical system failures should emphasize safe recovery.

The vehicle management system should be capable of changing IFF modes to indicate the presence of a critical system failure.[1]

These guidelines can be traced to Contingency Management System Level Requirements 1, 2, 3, 4, 5 and 6.

D-8 ABNORMAL/EMERGENCY TERMINATION OF FLIGHT

Abnormal and Emergency Termination of Flight should be mitigated in such a manner that the aircraft will be recoverable and/or will not cause loss of life or damage to property.

Emergency termination of flight should be considered a last resort for unmitigated failures. Termination of flight is defined as cessation of current flight operations either by landing at the nearest suitable air field or appropriate ditching area, or terminating flight operations via UAS internal explosive devices, or recovering via a parachute, or another means appropriate to the UAS design (i.e. autorotation for rotorcraft). Thus, "termination of flight" does not necessarily mean destruction of the aircraft.

As a guideline, emergency termination of flight should be considered when the UAS has experienced one or more of the following:[25]

1. Loss of or significant reduction in control
2. Un-extinguishable fire (engine, fuel system, electrical, hydraulic)
3. Severe loss of structure which impairs the ability to land or ditch the aircraft
4. Loss of link and communication with aircraft for a prolonged period and when an automatic landing is not an option.
5. When a suitable recovery location is not available.

Contingency management for abnormal termination of flight should include the following categories:

1. Structural failure
2. Fuel system failure
3. Hydraulic system failure

[25] A landing termination is adequate with reliability certified comparable to manned aircraft.

4. Electrical system failure
5. Foreign Object Damage (FOD)

Mitigation strategies for abnormal failures should be created to manage singular known events and multiple events such as a propulsion system failure which may perpetuate other multiple system failures.

These guidelines can be traced to Contingency Management System Level Requirements 1, 2, 3, 4, 5 and 6.

The Contingency Management System Level Requirements referenced above in each system failure section are listed below. Rationale and background information for each of these requirements are described in the CM requirements parent document (current version).

Table 2 System Level Requirements

1.	The UAS System shall be capable of performing contingency management to reduce the likelihood of loss-of-life or damage to personal property at a level of safety equivalent to manned aircraft.
2.	The Air Vehicle Element shall operate safely and predictably while performing emergency procedures.
3.	In the presence of failures and abnormal events that degrade continuous and full time pilot control of the UAS, the Contingency Management System shall provide related means to reduce the likelihood of loss-of-life or damage to personal property.
4.	In the presence of failures and abnormal events that degrade SA (Situational Awareness) of the UAS, Contingency Management shall provide related means to mitigate and circumvent in order to reduce the likelihood of loss-of-life or damage to personal property.
5.	As part of any Contingency Management activity, the UAS System shall always have a recovery location identified in any route it may be flying.
6.	The UAS System shall always have the means to safely terminate flight.

Appendix E
Weather Issues

(This Appendix will be provided with Revision G)

Appendix F
Control Station Abnormalities

F-1.0 EXECUTIVE SUMMARY

The AVCS (Air Vehicle Control Station) is a segment in the UAS (Unmanned Aircraft System). Other segments of the UAS are the UA (Unmanned Aircraft) and the C3 (Command, Control, and Communications) segment.

The AVCS performs a multitude of function that are described in other Access5 documents. Only a small sub-set of those functions are critical to the safe operation of the UAS.

The only critical functions in the AVCS are:

"Send commands to the aircraft"
and
"Receive health and status information from the aircraft"

Man-In-The-Loop (MITL) is the assumed control method. The criticality of the two functions will change as the autonomy levels of the UA increase above the MITL level.

The two Contingency Management requirements that apply to the two critical functions are:

> ***Continuous Pilot Control.*** *In the presence of failures and abnormal events that degrade continuous and full time pilot control of the UAS, the Contingency Management System shall provide related means to reduce the likelihood of loss-of-life or damage to personal property.*
>
> ***Situational Awareness****. In the presence of failures and abnormal events that degrade SA (Situational Awareness) of the UAS, Contingency Management shall provide related means to mitigate and circumvent in order to reduce the likelihood of loss-of-life or damage to personal property.*

F-2.0 BACKGROUND AND STATEMENT OF THE PROBLEM

F-2.1 Access5 is a NASA funded program that has the goal of facilitating integration of Unmanned Aircraft System (UAS) into the NAS (National Airspace System). A consortium of UAS industry members and NASA Research Center members who are tasked with formulating requirements and performing simulations and flight tests, results of which will be presented to the FAA. The FAA will use those inputs in forming up policy, procedures, and criteria for certification of UAS. The ultimate objective is to allow the UAS to file and fly in the NAS with a level of safety equivalent to manned aircraft.

Contingency Management concepts are described in the main body and in previous appendices to the document. This appendix has been created to describe how the Contingency Management Requirements are applied to the AVCS (Air Vehicle control Station).

F-2.2 Question to be answered by this analysis. "Which of the AVCS functions are Critical to the safe operation of the UAS and what are the Contingency Management requirements to mitigate failure of those critical functions".

F-2.3 Process used to arrive at the findings and conclusions.

F-2.3.1 Evaluated the total functions of the UAS. According to the literature,

> *Functional analysis begins with the identification of top level functions and ends with the allocation of those functions to lower level elements within the system.*[26]

One method for performing this first step is fairly simple, go to the Access5 Functional Requirements Document (FRD) and repeat the four main functions a UAS must perform: Aviate, Navigate, Communicate, Avoid hazards. [27]These four top level functions are the baseline functions of the UAS and from there, subsequent functions are created in order to satisfy the top level ones.

In practice, an architecture is often envisioned much before the actual functions are completely identified and analyzed in detail. This has been the case with Access5, in that a UA (architectural solution) and the AVCS (architectural solution) and the C3 (architectural solution) were identified as the three segments of the UAS from the very beginning. This is to be expected mainly because several fielded UAS continually serve as examples, having been developed with that architecture.

F-2.3.2 Narrowed the scope to AVCS Critical Functions.

A detailed analysis of the traceability of segment requirements to the FRD functions is not in the scope of this appendix. What is in the scope is to look at the functions of the AVCS segment as they are currently envisioned, and determine which of the AVCS functions are critical. (Identifying the critical functions for all three segments is also not in the scope of this appendix). The AVCS critical functions will be identified so they can be discussed in detail, and thus enable creation of contingency management requirements.

A primary premise of this analysis is that the top level UAS function must be performed by one or more of the segments. Select any of the FRD functions and attempt to trace down to which of the segments is performing that function. Most of the instances show traceability to all three of the segments. For example, the communicate function appears to be primarily performed by the C3 segment, but in actual practice, all three segments are involved with the communicate function. It appears that the aviate function is primarily performed by the UA segment, but that may not be true if the UA is primarily flown by a Man-in-The-Loop (MITL), in which case the C3 and the AVCS are heavily involved.

F-2.3.3 Created Contingency Management requirements concerning AVCS abnormalities.

F-3.0 ANALYSIS OF UAS FUNCTIONS

F-3.1 Discussion of UAS functions in general. All functions of the UAS are performed by one or more of the segments. In some UAS functions, where responsibility for performance of the function is shared, one segment may have a more significant role than any of the others. For example, with the navigate function, the autonomous UA is responsible for the entire navigate function while the AVCS (pilot) is relegated to a monitor role. Although the bread and butter of performing the navigate function is done by the on-board navigators, the pilot still must monitor to be sure the route is being followed in accordance with his requirements. So, the AVCS has a navigate function as well as the UA, however the UA has a much larger part of the function, especially in autonomous aircraft.

---

[26] Systems Engineering Management Guide; Pg. 6-1

[27] Access5 Functional Requirements Document. March 2005.

Same concept applies concerning the involvement of the C3 segment in the Aviate function. In a predominant MITL design, the AVCS and the C3 have aviate functions that are as important as those performed by the AV segment.

F-3.2 Critical functions discussion and definitions. Most important about the premise stated above is that not all functions performed by each of the segments is critical. Some may be extremely important to the mission of the UA, but they may not be critical as can be seen in the following definitions:

RTCA/DO-178A dated March 22, 1985, "Software Considerations in Airborne Systems and Equipment Certification," defines certain terms to classify the criticalities of functions.

> *Failure conditions adversely affecting non-essential functions would be minor,*
> *Failure conditions adversely affecting essential functions would be major, and*
> *Failure conditions adversely affecting critical functions would be catastrophic.*[28]

Critical is defined as:

> *Indispensable to the operation of a machine.* [29]

A Critical Function is defined elsewhere as:

> *A function whose loss would prevent the continued safe flight and landing of the airplane. Note: The term "Critical Function" is associated with a Catastrophic Failure Condition.*[30]

SIMPLE INTERPRETATION. If the function is not available for any reason, and the UAS experiences a catastrophic event because that function is not available, then that function is a critical function.

Now comes the challenge of defining a "CATASTROPHIC" event for the UAS. So far all definitions for catastrophic have been oriented toward multiple fatalities of the occupants, or incapacity for continued safe flight and landing while occupants are strapped into seats. Catastrophic certainly does not apply to UAS when talking about multiple fatalities of occupants, and may not be accurate when talking about safe flight and landing with expendable UAS aircraft.

Functions may be critical for the UAS at the systems level, so therefore one or more of the segments has a contribution that is also a critical function. The following three diagrams depict the concept of critical functions at the segment level.

---

28 RTCA/DO-178A

29 Webster's Ninth New Collegiate Dictionary. 1989, Merriam-Webster Inc.; Pg 307

30 Advisory Circular 23.1309-1C Equipment Systems and Installations in Part 23 Airplanes. March 12, 1999 Par 6i

This model shows that all 3 Segment contributions to UAS function X are required for UAS function X to be successful. Corollary is if any of the three functions performed by the segments fails, then the UOS function fails.

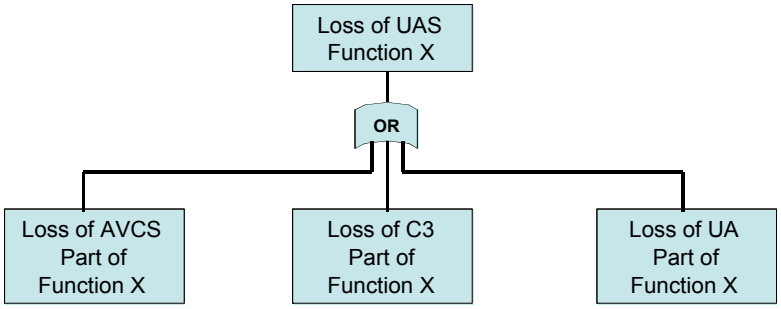


Figure F-3.2a Any of the Three Segments can experience a Critical Failure of any of the Three Segments Which Causes a UAS Critical Failure.

This model shows that 2 Segments contribute to UAS function Y. Both are required for UAS function Y to be successful. Corollary is if any of the functions performed by the segments fails, then the UOS function fails.

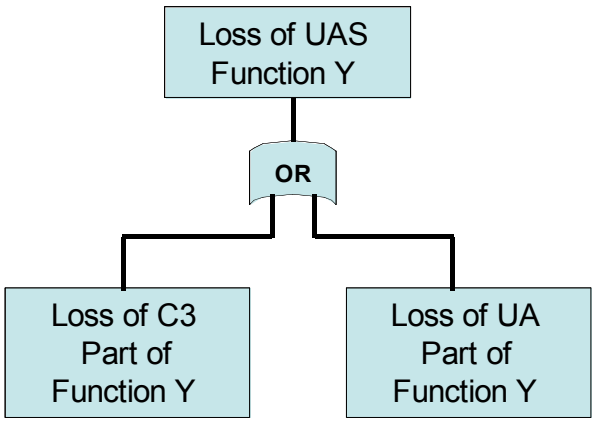


Figure F-3.2b. A Critical Failure in Either of Two Segments causes a UAS Critical Failure

This model shows that when one segment is performing the UAS function exclusively, then if the segment function fails, the UAS function will fail.

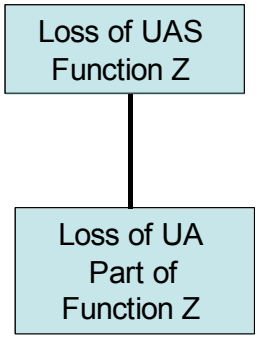


Figure F-3.2c. Single Segment Critical Function

F-3.3 Functions that are unique to the UAS. The UAS (at the systems level), has additional functions that are not found in manned aircraft. Most significant of those exclusive functions is the function that roughly equates to: FLY THE AIRCRAFT FROM A POSITION OUTSIDE OF THE AIRFRAME. That function itself has a lot of involvement by all three segments, from data links, to displays, to cockpit controls and many others. As conditions, technology, environments evolve, so will the gradual and inevitable migration of the ability to control aircraft away from the manned cockpit. For now though, that subject will not be addressed, since the entire manned aircraft community, with the responsibility for safety of passengers, has a responsibility to have the final say on everything that the aircraft does or is told to do.

F-3.4 Impact of Autonomous functions in Unmanned Aircraft.

C2 comes from somewhere, it may be from a computer on the aircraft, or it may come from the Man-In-The-Loop (MITL) who is in the AVCS. Several points come to mind when this viewpoint is analyzed.

In order for the MITL to modify the behavior of the UA, or to command it to take an action he must have a functioning Command Chain, which is the end-to-end path of the command from mouse click to control surface movement. This function is "Command The UA" or in the environment of autonomous aircraft, "Modify The Behavior of the UA".

Autonomous aircraft have less reliance on a control station and in the future, may not need one at all. For the time being, and for purposes of this appendix, MITL will be the primary means of control.

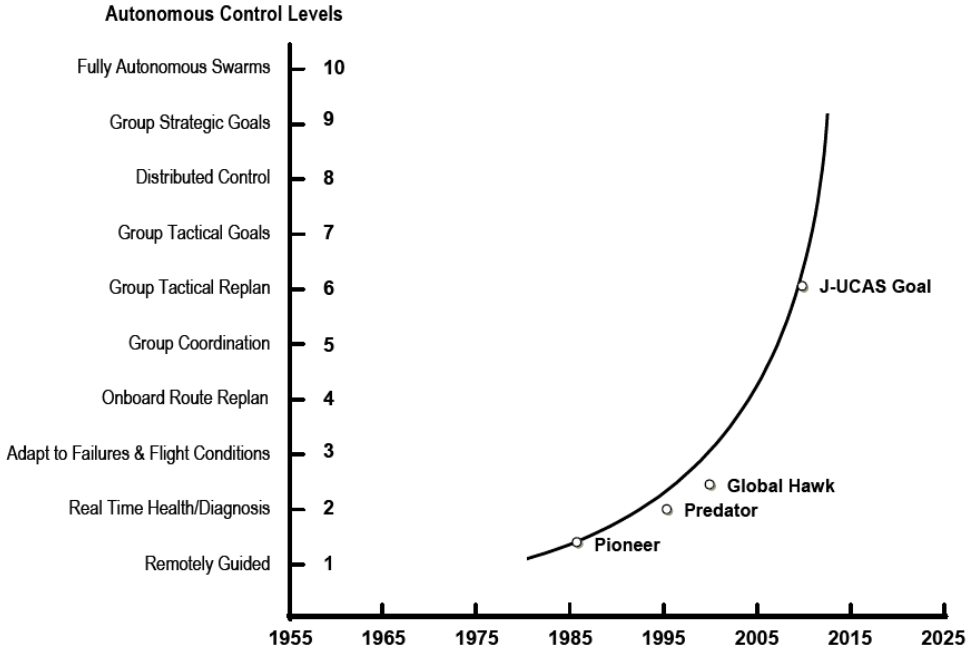


Figure F-3.4 Diagram courtesy of "Unmanned Aircraft Systems (UAS) UAS Roadmap" 2005 2030[31]

Military systems use autonomous functions in the "Dull, Dirty, Dangerous" tasks that are characteristic of military applications of UAS. The chart above depicts the time frames that these autonomous functions are expected to emerge as operational capabilities. Civil systems will utilize autonomous systems with some capabilities that are similar up to a certain point. Above that point, the requirements will dictate how advanced a particular UAS must be with regards to level of autonomy. An example would be Autonomous Control Level (ACL) 6, where the Group Tactical Replan functions would be utilized in police and disaster relief activities. That level may not be used if the UAS has a transportation function.

For Step one of Access5, the immediate requirement is to expect at least Autonomy level 5 (Group Coordination) to account for the Sense and Avoid function. Any level of autonomy

31 UAS Roadmap 2005; C-14

above that level would need coverage in later steps of Access5. For additional information on autonomy see the UAS roadmap 2005 Appendix A Overview.[32]

F-3.5 Summary of analysis already completed by other Work Packages.

The objective of functional analysis in many systems is to fully dissect the functions of a system in what is typically called functional decomposition. In a textbook development program the functional flow will start at the highest level, and flow to lower tiers to identify how a system works in terms of functional descriptions. From there, requirements evolve and the development continues.

The Charter of Access5 calls for requirements exclusively as a descriptor for the functions, this seems to have served the objectives of Access5 quite well. For example, the Work Packages present specialty functions in terms of requirements that they must perform. Functional analysis serves a very important role in getting to those requirements, and looking at the H S I results, it appears that extensive effort and resources were invested in determining what the functions of an AVCS are. The linkage between these functions and the final requirements will be traceable. All Work Package products roughly follow a similar mold, where the top level functional requirements are identified for their discipline.

An additional dimension is needed in order to better describe the importance or priorities of the functions in the UAS. That added dimension in inherent in the criticality of those functions.

The analysis will identify the critical functions in the AVCS so that contingency management requirements and guidelines can be formulated. Not every function (Critical and non-critical) of the AVCS was analyzed in detail. Although a small subset of non-critical functions were touched, the total inventory of non-critical functions is too extensive for serious consideration and analysis. The critical functions have been identified, and placed into categories that summarize the similar features. In the following tables those are called the "Summary Critical Functions". This strategy is appropriate at this level to get a feel for which of the critical functions can be identified with a common thread.

F-3.5.1 Functions of the AVCS from the H S I Work Package perspective.

Command and Control Functional Requirements are described in the H S I Work Package deliverable as:

> *Beginning with HSI high-level functional requirements for Contingency Management, and Contingency Management technology elements, HSI requirements for the interface to the pilot were identified. Results of the analysis describe (1) the information required by the pilot to have knowledge of system failures and associated contingency procedures, and (2) the control capability needed by the pilot to obtain system status and procedure information. Fundamentally, these requirements provide the candidate Contingency Management technology concepts with the necessary human-related elements to make them compatible with human capabilities and limitations. The results of the analysis describe how Contingency Management operations and functions*

[32] UAS Roadmap 2005.

should interface with the pilot to provide the necessary Contingency Management functionality to the UA-pilot system.[33]

The following table summarizes the top-level functional requirements of the H S I in Access5. This is a list of functions that the AVCS will perform, as depicted in the H S I Work Package deliverable document.[34] The H S I document does not specifically designate a Hazard Classification or label any of the functions as critical. The purpose of this study was to identify critical functions of the AVCS. The last 4 functions do not fit the criteria of critical because failure does not necessarily cause a catastrophic event.

Functions of the UAS From the HSI Work Package Perspective	***Summary Critical Function***	***Required for the UAS Function:***
Enable the pilot to update the UAS's flight plan	C2 Uplink	UA, AVCS, C3
Enable the pilot to command flight maneuvers		UA, AVCS, C3
Convey information to the pilot to monitor flight maneuvers	C2 Downlink	UA, AVCS, C3
Convey information to the pilot to determine the health and status of the UAS		UA, AVCS, C3
Convey information to the pilot to determine the unmanned aircraft's position, heading, course, speed, and altitude		UA, AVCS, C3
Enable the pilot to communicate with ATC	Situational Awareness (Not a critical Function)	AVCS, C3
Convey information to the pilot to avoid cooperative aircraft		AVCS, C3
Convey information to the pilot to avoid hazardous weather		AVCS, C3
Enable the pilot to manage contingencies		AVCS, C3

GH Functions.xls

Figure F-3.5.1 H S I High level Functional Requirements. [35]

Look at each of the four functions that are judged to not be critical. For the first, (Enable the pilot to communicate with ATC), ask what is the threshold that determines when the Pilot to ATC communications link becomes a flight critical function? The Communicate and the Avoid Hazards requirements from the Access5 FRD appear to provide guidance and traceability for the ATC functional Requirements found in the table above. If the ATC communications fails with no other abnormal events such as any under the FRD requirement "Avoid Hazards", then the ATC communications function all by itself does not appear to fit the Flight Critical Function definition.

The second function (Convey information to the pilot to avoid cooperative aircraft), will fit the criteria if the function is lost, and that loss causes a catastrophic event. In the case where the ATC agency is not able to talk with the UAS pilot to divert for traffic avoidance, and the other aircraft is not able to divert, that scenario is a multiple failure that would not be considered a single failure (loss of function), but would be considered loss of two unrelated functions at the same time. The two failures would be loss of ability to divert aircraft A and loss of ability to

[33] H S I Pilot-Technology Interface Requirements for Contingency Management. August 31, 2005; Executive Summary

[34] H S I Pilot-Technology Interface Requirements for Command, Control, Communications. August 31, 2005.. Executive Summary.

[35] H S I Pilot-Technology Interface Requirements for Contingency Management. August 31, 2005; Executive Summary

divert aircraft B. (Multiple failures are discussed in an earlier appendix). Multiple failures have been discussed extensively on an informal basis in Access5 and the conventional wisdom is that they are too rare to command any serious discussion. Footnote text message. (Author's personal observation, not an Access5 position)

The UAS world is very sensitive to the requirement for collision avoidance. Any topic or discussion that suggests that failures of the function "Avoid collisions with a manned aircraft" is to be treated lightly, would be a mistake. However, many factors will have to be considered before this function is labeled a flight critical function, such as autonomy levels of the UAS in the see and avoid activity. Even under the current MITL environment, the ability for ATC to contact the pilot should be seriously evaluated to determine if the multiple paths available may make this failure improbable. So for purposes of this document, the function "Enable the pilot to communicate with ATC" is NOT a critical function.

The third function (Convey information to the pilot to avoid hazardous weather) is also not considered a critical function. The multiple paths for the pilot to gain information on weather makes loss of this function improbable.

The fourth function (Enable the pilot to manage contingencies) is considered to be inherent in the C2 Uplink and C2 downlink critical functions. This function by itself does not fit the Critical definition.

F-3.5.2 Functions of the AVCS from the Reliability Work Package perspective.

F-3.5.2.1 Functional hazard Analysis in-work by the Reliability Work Package.

The FHA presently in work is summarized in an MS Excel© spreadsheet table created by the Reliability Work Package.[36] The FHA worksheet shows 115 separate functions of a UAS, and each function lists anywhere from zero to 6 failure conditions. The total number of Functional Hazards is 425, one per row of the worksheet. The figure below shows the main column headings.

Record Number	Function	Flight Phase	Failure Conditions	Operational Consequences (effect of failure on UAS)	Hazard Classification (Criticality)	Remarks

Figure F-3.5.2a Headers Used by the Reliability Work Package in Their FHA

Every Functional Hazard has a Hazard Classification assigned. Those Hazard Classifications are from AC23.1309-1C. The Hazard Classifications are Catastrophic, Hazardous, Major, and Minor. Only the definition of Catastrophic is repeated, since contingency Management is only concerned with the critical functions and therefore the catastrophic hazard classifications.

> *Catastrophic: Failure Conditions that are expected to result in multiple fatalities of the occupants, or incapacitation or fatal injury to a flight crewmember normally with the loss of the airplane. Notes: (1) The phrase "are expected to result" is not intended to require 100 percent certainty that the effects will always be catastrophic. Conversely, just because the effects of a given failure, or combination of failures, could conceivably be catastrophic in extreme circumstances, it is not intended to imply that the failure condition will necessarily be considered*

[36] Access5 Step 1 FHA Master 050815.xls (Preliminary Considerations for UAS Reliability for Experimental Certification). August 8, 2005

catastrophic. (2) The term "Catastrophic" was defined in previous versions of the rule and the advisory material as a Failure Condition that would prevent continued safe flight and landing.[37]

F-3.5.2.2 Summary of the critical functions as identified in the FHA are shown in the following table. This is a list of all of the functions that the Reliability Work Package identified as critical (leads to Catastrophic Hazard Classification) for the UAS when the AVCS is involved in performing that function. UAS functions that do not involve the AVCS are not shown.

There are a total of 23 functions that the FHA identifies as critical. However, only 8 appear to comply with the definition of critical, those are the ones that are summarized by the C2 Uplink Summary Critical Function and the C2 Downlink Summary Critical Function.

Fifteen functions are related to Situational Awareness. Those are judged to not be critical, rationale for not considering them critical is the same as was explained in Par F-3.5.1 above concerning the H S I functions.

Critical Functions of the UAS From the Reliability Work Package Perspective	***Summary Critical Function***	***Required for the UAS Function:***
Execute comand to control environmental conditions inside the UAS	**C2 Uplink**	UA, AVCS, C3
Execute Corrective Action Command		UA, AVCS, C3
Execute power subsystem command		UA, AVCS, C3
Execute speed change command - includes thrust reversers, etc.		UA, AVCS, C3
Execute the center of gravity command		UA, AVCS, C3
Convey state of center of gravity	**C2 Downlink**	UA, AVCS, C3
Convey state of environment inside the UAS		UA, AVCS, C3
Convey State of UAS Power Subsystems		UA, AVCS, C3
Convey relative location of adverse environmental conditions	**Situational Awareness (Not a Critical Function)**	AVCS, C3
Convey relative location of Ground Path Obstruction		AVCS, C3
Assess adverse environmental conditions		AVCS, C3
Assess collision potential		AVCS, C3
Convey air traffic tracks		AVCS, C3
Detect adverse environmental conditions		AVCS, C3
Detect air traffic		AVCS, C3
Detect Ground Path Obstructions		AVCS, C3
Evaluate collision potential		AVCS
Prioritize adverse environmental conditions		AVCS
Prioritize collision threats		AVCS
Prioritize potential collision threats		AVCS
Track air traffic		AVCS
Track relative location of adverse environmental conditions		AVCS
Track relative location of Ground Path Obstruction		AVCS

Kelly's FHA.xls

Figure F-3.5.2b. Critical Functions of the UAS From the FHA

F-3.5.3 Functions of the AVCS from the Fielded Systems perspective.

The table shown next is a summary level compilation of the functions a typical fielded AVCS performs. Keep in mind that some of the actual functions may not be seen in the table but

[37] Advisory Circular 23.1309-1C Equipment Systems and Installations in Part 23 Airplanes. March 12, 1999. Par 6t. The strict definition of catastrophic has to be refined to accommodate characteristics of the UAS concerning occupants. Is one fatality on the ground catastrophic? Is destruction of an expendable UAS catastrophic?

they are subsequent to one of those shown. (Man-In-The-Loop method is assumed, meaning the UA is being flown manually.

This is a list of the UAS functions when the AVCS is involved in performing that function. Functions that do not involve the AVCS are not shown. UAS is assumed to be flown manually so the results shown will roughly correlate with other data from this document.

Two functions are related to Situational Awareness. Those are judged to not be critical, rationale for not considering them critical is the same as was explained in Par F-3.5.1 above concerning the H S I functions.

Functions of the UAS From a Fielded UAS Perspective	***Summary Critical Function***	***Required for the UAS Function:*** ***(UA, AVCS, C3)***
Send command to the UA	C2 Uplink	UA, AVCS, C3
Divert the UA to a different route		UA, AVCS, C3
Receive signals from the UA	C2 Downlink	UA, AVCS, C3
Display aircraft performance parameters		UA, AVCS, C3
Notify pilot when UA is malfunctioning		UA, AVCS, C3
Receive/display status from UA		UA, AVCS, C3
Enable pilot to/from ATC voice communications	Situational Awareness (Not a Critical Function)	AVCS, C3
Receive diversion information from ATC		AVCS, C3

GH Functions.xls

Figure F-3.5.3 Functions of the UAS From the perspective of a fielded UAS

F-4.0 ANALYSIS OF AVCS CONTINGENCIES

F-4.1 Discussion on losing a function in the AVCS. For purposes of this discussion, loss of a function is synonymous with failure of the function. Loss of the function is preferred wording because that is the end result of a failure; the ultimate effect is that the function is no longer available. This concept (loss of function) assumes redundant features to supply the function have already been expended and there are no additional methods available to restore the function. Either that or the function is simply not important enough to cause any concern if it is lost. Volumes are available concerning techniques designers can use to prevent loss of function, including probabilistic methods.

F-4.2 Loss of non-critical function: This is the loss of a function that is not critical, such as creating a mission plan, maintain AVCS environment, storing images etc. This type of loss normally will not cause a catastrophic event if it occurs.

F-4.3 Loss of critical function: The effect of loss of a critical function is that a catastrophic event will occur if the function is no longer available.

F-4.4 Functions of the AVCS that are critical to the safe operation of the UAS. Critical functions in the UAS have been identified. There are two main categories of critical function as determined in the tables above. They are:

A. C2 Uplink functions,

B. C2 downlink functions,

F-5.0 AVCS CONTINGENCY MANAGEMENT REQUIREMENTS TO MITIGATE FAILURES OF THE CRITICAL FUNCTIONS IN THE AVCS.

F-5.1 Top level contingency management requirements have been formulated and presented in the main part of this document. The CM requirements that apply to the critical functions of the AVCS are already identified and are part of those UAS requirements. Those two requirements are:

> *4.3.1.1.2 Continuous Pilot Control. In the presence of failures and abnormal events that degrade continuous and full time pilot control of the UAS, the Contingency Management System shall provide related means to reduce the likelihood of loss-of-life or damage to personal property.*
>
> *4.3.1.1.3 Situational Awareness. In the presence of failures and abnormal events that degrade SA (Situational Awareness) of the UAS, Contingency Management shall provide related means to mitigate and circumvent in order to reduce the likelihood of loss-of-life or damage to personal property.*

F-5.2 AVCS guidelines for Contingency Management have been formulated to specifically address the critical functions in the AVCS.

F-6.0 BIBLIOGRAPHY

1. *UAS Roadmap 2005*

2. *Advisory Circular 23.1309-1C Equipment Systems and Installations in Part 23 Airplanes.* March 12, 1999

3. *Advisory Circular 25.1309-1A System Design and Analysis.* June 21, 1988.

4. *Mil-Std 882C Military Standard System Safety Program Requirements.* 19 January 1993.

5. *H S I Pilot-Technology Interface Requirements for Contingency Management*. August 31, 2005.

6. *H S I Pilot-Technology Interface Requirements for Collision Avoidance*. August 31, 2005.

7. *H S I Pilot-Technology Interface Requirements for Functional Requirements Document*. August, 2005

8. *H S I Pilot-Technology Interface Requirements for Command, Control, Communications*. August 31, 2005.

9. A*ccess5 Step 1 FHA Master 050815.xls (Preliminary Considerations for UAS Reliability for Experimental Certification)*. August 8, 2005.

10. *Webster's Ninth New Collegiate Dictionary*. 1989, Merriam-Webster Inc.

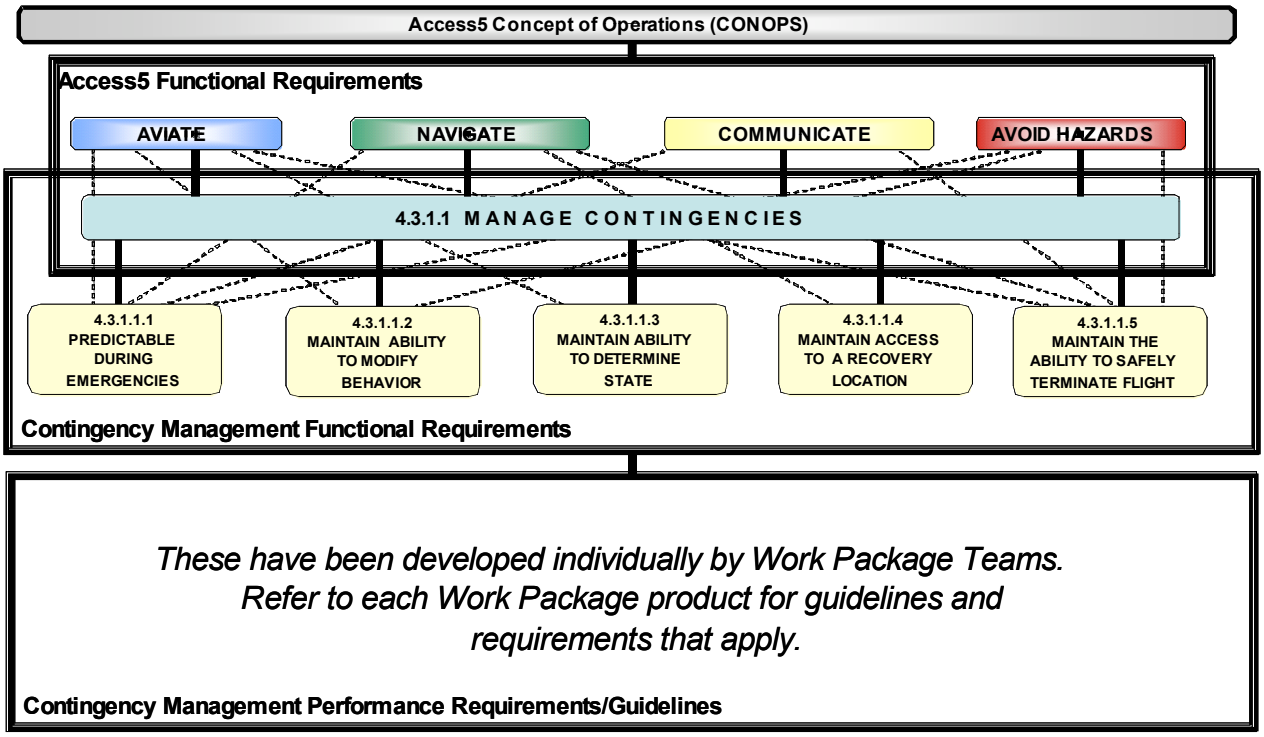
11. *RTCA/DO-178A* dated March 22, 1985.

12. *Systems Engineering Management Guide. Defense Systems Management College*. January 1990.

13. *Open Systems and the Systems Engineering Process. Michael Hanratty, Robert H. Lightsey, Arvid G. Larson*. Acquisition Review Quarterly. Winter 1999.

14. *Access5 Functional Requirements Document*. March 2005.

Appendix G
Traceability of CM Requirements to the Access 5 Functional Requirements Document



Individual work packages have developed Performance Requirements/Guidelines that trace to the Access5 Functional Requirements Document through the path that defines their specialized functions. Some of those same Performance Requirements/Guidelines are related to Contingency Management and thus have similar traceability to the FRD through the Contingency Management Work Package Functional Requirements.